INSTRUCTIVO PARA LA IMPLEMENTACIÓN EFECTIVA DE SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS SIEM PARA LA AGENCIA NACIONAL DE LA SUPERACIÓN DE LA POBREZA EXTREMA ANSPE

JOHN WILSON PEÑA NINCO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2015

INSTRUCTIVO PARA LA IMPLEMENTACIÓN EFECTIVA DE SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS SIEM PARA LA AGENCIA NACIONAL DE LA SUPERACIÓN DE LA POBREZA EXTREMA ANSPE.

JOHN WILSON PEÑA NINCO

Trabajo de grado para optar al título de
Especialista en Seguridad Informática

Asesor
CESAR IVÁN RODRÍGUEZ
Ingeniero Electrónico

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2015

Nota de Aceptación

_____

_____

_____

_____
Firma director del proyecto

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, D.C., Julio de 2015.

DEDICATORIA

A ellas quienes siempre están ahí incondicionalmente cuando necesito su apoyo.

A él por motivarme a cumplir mis retos y enseñarme a vivir.

Quiero agradecer a mi familia por su apoyo y motivación en especial a la mujer que me acompaña en todo momento y con quien cuento incondicionalmente.

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Al ing. Cesar Iván Rodríguez, asesor del proyecto

A la Universidad Piloto de Colombia

Son muchas las personas que forman parte de mi vida profesional a todas ellas quiero agradecer su apoyo y enseñanzas.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ANTIVIRUS: programa que detecta la presencia de un virus y puede neutralizar sus efectos.[1]Se puede decir que es un software que está permanentemente monitoreando y analizando el contenido de la información y programas que están en la memoria del computador, así como sus dispositivos periféricos y conexiones de red e internet en búsqueda de archivos conocidos como malware, que buscan causar fallas, deteriorar la información o el acceso que se tiene en los dispositivos de los usuarios y de la red de la entidad.

CONFIDENCIALIDAD: cualidad de confidencial.[2] Se puede decir en un entorno informático que los recursos del sistema solo deben ser accedidos por las partes autorizadas.

DLP: acrónimo de Data Loss Prevention hace referencia a los sistemas que identifican, monitorean y protegen los datos en uso, en movimiento y reposo, por medio de la inspección profunda de contenidos, con el objetivo de detectar y evitar el uso no autorizado de la información.[3]

DISPONIBILIDAD: cualidad o condición de disponible[4]. En un entorno informático se puede decir que los recursos del sistema deben permanecer accesibles por las partes autorizadas.

FIREWALL: dispositivo que realiza la función de separar las maquinas internas de la red, con la red externa bajo el control del administrador de la consola. Actúa como punto central para permitir el acceso a los servicios en la red interna por parte de los usuarios o maquinas fuera de la red[5].

INTEGRIDAD: cualidad de integro. En un entorno informático se puede decir que los elementos del sistema solo pueden ser modificados por las partes autorizadas.[6]

---

[1] RAE. Real Academia Española. Definición de antivirus. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://lema.rae.es/drae/?val=antivirus

[2] Ibid.

[3]ROEBUCK, Kevi. Data Loss Prevention DLP: High-impact Strategies – What You Need to Know. Emero Pty Limited. 2011. 80 p,

[4] REAL ACADEMIA ESPAÑOLA. Disponibilidad. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://lema.rae.es/drae/?val=disponibilidad

[5] KRUEGEL, Chris et al, intrusion detection and correlation: Challengeds and solutions, Santa Barbara, California, USA. Springer, 2005. p.2.

[6] REAL ACADEMIA ESPAÑOLA. Integridad. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://lema.rae.es/drae/?val=integridad

ITIL: marco que describe las mejores prácticas en la administración de servicios de tecnologías, se enfoca en la continua medición y mejoramiento de la calidad de los servicios entregados por el área de TI.[7]

LEM: acrónimo de Log Event Manager hace referencia a la solución de herramienta de correlación de logs del fabricante Solar Winds.

LOGS: registro oficial de un evento durante un periodo de tiempo en particular, es usado para registrar datos o información sobre quién, cuándo y por qué un evento ocurre en un dispositivo en particular o en las aplicaciones que se encuentran en estos dispositivos[8].

MALWARE: es cualquier software o programa que causa daño a un usuario, computador o red[9].

SIEM: acrónimo de Security & Information Event Manager, son herramientas que proporcionan los medios para analizar en tiempo real los eventos de seguridad, así como los medios de reporte y almacenamiento de estos, permiten la visualización de los eventos por un periodo de tiempo.[10]

SGSI: acrónimo de Sistema de Gestión de Seguridad en la Información. Está compuesto por un conjunto de políticas que definen la administración de la seguridad de la información en Colombia. Aplica controles, normas y estándares como la ISO27000.

SNMP: acrónimo de Protocolo Simple de Administración de Red por sus siglas en inglés, es un protocolo creado para consultar y configurar los dispositivos y las tramas. SNMP son mensajes que se generan en un dispositivo cuando ocurre un evento en particular.

SYSLOG: "Syslog es un sistema de logs que se encarga principalmente de la administración de logs, los cuales son generados por eventos del sistema, sus programas o por el Kernel."[11]El termino syslog es utilizado a menudo para describir

---

[7] ITIL como apoyo a la seguridad de la información. [En línea]. [Noviembre 2014] disponible en: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/04-ITILSoporteSGSIBasadoISO27001.pdf

[8]BABBIN, Jacob et al, Security log managment. Singress. Walthan, MA, USA, 2013. p 4.

[9]SIKORSKI, Michael. Practical Malware Analysis. No strach press. San Francisco, CA. USA. 2012. p.28

[10] CHUVAKIN, Anton et al. Logging and log Management. Syngress. Walthan. MA. USA. 2013. p. 119

[11]TORRES, Juan Carlos; RONDÓN, Richard "Control, Administración e Integridad de Logs." [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: en:http://www.criptored.upm.es/guiateoria/gt_m248h.htm

tanto el protocolo para el envío de mensajes, como el programa o librería que envía mensajes.

TRAP: alarma generada por el sistema para reportar ciertas condiciones o cambios de estado a un proceso.[12]

12 VICENTE, Carlos. “Gestión de Traps SNMP” [en línea], [Consultado el 23 de octubre de 2014]. Disponible en: https://www.nsrc.org/workshops/2008/walc/presentaciones/gestion_traps.pdf

RESUMEN

En este documento se presenta la propuesta para la implementación de una herramienta de gestión de eventos y seguridad de la información SIEM, en la Agencia Nacional para la Superación de la Pobreza Extrema - ANSPE, el cual pretende dar a conocer al lector el funcionamiento técnico y las características a tener en cuenta en el momento de realizar la instalación y configuración de este tipo de herramientas.

Contiene las diferentes fases para realizar la implementación de la herramienta LEM del fabricante Solar Winds, con la cual cuenta la ANSPE. Brinda una explicación técnica del dispositivo, así como la descripción de la selección de los dispositivos y fuentes de información que serán analizados, con el fin de monitorear los eventos que estos presenten. Al finalizar se describe la configuración de la herramienta en la entidad.

Palabras clave: herramienta gestión de eventos, administración, dispositivos.

INTRODUCCIÓN

El crecimiento de los delitos informáticos, ha generado que las entidades gubernamentales se vean en la necesidad de contar con una tecnología vigente, con el fin de garantizar la operación y cuidar la información vulnerable que estas manejan.

Las entidades en el afán de proteger la información, cuenta con dispositivos y herramientas de seguridad como lo son antivirus, Firewall y configuraciones en los equipos de red y servidores. No obstante, todos estos componentes suministran una serie de reportes de la operación, demandando se realice el respectivo análisis.

Este proyecto está orientado a la elaboración de un documento guía que facilite implementar una herramienta para correlacionar eventos, lo que permitirá al grupo de seguridad de la entidad aumentar su nivel de protección, mitigar riesgos, disminuir el margen de error y optimizar los tiempos dedicados a esta labor.

1. PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La creciente tendencia de los ataques informáticos a las entidades del estado, eleva la preocupación de proteger la información vulnerable de las mismas, lo cual es mitigado en una primera instancia con los dispositivos de seguridad y de red, sin embargo con esto nace la necesidad de administrar óptimamente los reportes entregados por dichos equipos.

El monitoreo de los logs que se generan en los dispositivos es una actividad que por lo general la realiza el oficial de seguridad de manera manual, aumentando el margen de error por la cantidad de información a verificar, exponiendo a que se puedan pasar por alto posibles ataques. Así mismo, mal gastando el recurso humano en labores engorrosas que toman tiempo y no garantiza en un cien por ciento su efectividad.

¿Cómo se debe implementar una solución que facilite la gestión de los profesionales de seguridad de la información para analizar los log, eliminando tareas operativas y previniendo ataques o futuras anomalías, basados en el análisis y administración de los logs de los dispositivos?

1.2 JUSTIFICACIÓN

Una de las tareas más demandantes para un oficial de seguridad y la cual consume gran cantidad de tiempo es el monitoreo o análisis de logs de los dispositivos de la entidad, dado a la gran cantidad de equipos e información a analizar y la probabilidad de error humano.

Una forma eficiente para gestionar y analizar los eventos que registran los dispositivos de seguridad y de red de la entidad, es implementar un correlacionado de logs o eventos. Este tipo de herramienta permite analizar instantáneamente los logs, contar con un registro histórico de estos. Logrando una administración controlada de los eventos, que facilite tomar acciones inmediatas en el momento que se presenten ataques o fallas.

Es relevante identificar los dispositivos que van hacer parte de la herramienta, teniendo en cuenta cuales activos pueden ser los más críticos y demandan mayor información, realizando así un aprovechamiento óptimo de la herramienta.

1.3 OBJETIVOS

1.3.1 Objetivo general. Plantear el procedimiento para la implementación de una Herramienta de monitoreo y administración de log LEM (*Log Event Managment*) que complemente la solución SIEM (*System Information and Event Managment*) en la Agencia Nacional para la Superación de la Pobreza Extrema ANSPE.

1.3.2 Objetivos específicos.

- Describir el funcionamiento técnico de dispositivo LEM
- Definir condiciones para la implementación de herramienta SIEM
- Descripción técnica para la implementación de dispositivo LEM
- Identificar las anomalías que se presentan en los dispositivos.

1.3.3 Alcance. La clasificación del proyecto está en la línea de detección y auditoria dado que contempla el desarrollo de actividades necesarias para realizar la implementación de una herramienta de correlación de eventos (LOG´s).

Al finalizar el proyecto la ANSPE estará en capacidad de realizar la implementación de la herramienta SIEM, la cual le permitirá generar reportes para dar cumplimiento a los controles que se implemente de la norma 27002 y generar alertas para identificar los actores de comportamientos sospechosos.

1.4 LIMITACIONES

El proyecto es viable de desarrollo en cuanto la ANSPE cuente con SGSI funcional (probado), un organigrama de seguridad y del personal de seguridad, así como se encuentren definidos los activos de información y operación relevantes.

La ejecución del presupuesto en el presente documento abarca las condiciones necesarias para la implementación de la herramienta SIEM en la ANSPE, así como los parámetros para la configuración de alertas y mecanismo de monitoreo que se deben configurar en base a la matriz de amenazas. No están contemplados los planes de remediación o respuesta ante incidentes de seguridad o mal uso de las herramientas.

2. MARCO TEÓRICO

2.1 SEGURIDAD DE LA INFORMACIÓN

Mantener un nivel mínimo de protección de la información, custodiando la confidencialidad e integridad de la misma, es hoy en día una prioridad para cada una de las entidades estatales.

Seguridad de la información se puede definir como la custodia o protección ante los daños causados voluntaria o involuntariamente a los activos físicos o de data de una entidad.

La seguridad informática como fin principal tiene el deber de proteger la información mediante tres pilares que son integridad, confidencialidad y disponibilidad.

Dado que la información es el activo principal de la entidad y los usuarios son quienes consultan, modifican y hacen uso de esta, es de gran importancia velar por mantener un nivel alto de seguridad informática, implementado elementos de seguridad activa como son firewall, antivirus, políticas y elementos de seguridad pasiva tales como políticas de recuperación, almacenamiento de backup.

2.2 SEGURIDAD EN ENTIDADES DEL ESTADO

El Decreto 1151 del 14 de abril de 2008, establece los lineamientos generales que las entidades del Estado deben adelantar para la implementación de la Estrategia de Gobierno en Línea, la cual tiene como propósito el "Contribuir a la construcción de un Estado más eficiente, más transparente y participativo y que presta mejores servicios con la colaboración de toda la Sociedad, mediante el aprovechamiento de las TIC".[13]

Toda entidad del estado debe mantener un mínimo de normas de seguridad de la información, con el objetivo de conservar la confidencialidad, integridad y

[13] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Dirección de gobierno en línea. Decreto 1151 de 2008. Artículo 2. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://programa.gobiernoenlinea.gov.co/busquedas.shtml?apc=jxx;x;x;x1-&x=4480

disponibilidad de la información, por lo que se deben mantener los equipos y la red protegidos y aislados de ataques o vulnerabilidades**.**

2.3 GOBIERNO EN LÍNEA

"Tanto el documento CONPES 3072 de 2000 - Estrategia de Gobierno en Línea y los lineamientos del Plan Nacional de Desarrollo, ordenan a las entidades públicas del orden nacional utilizar el poder de las tecnologías de información y comunicaciones – TIC, para mejorar la eficiencia y transparencia de la administración pública"[14].

A su vez el Ministerio de Tecnologías de la Información y las Comunicaciones, establece mediante el Decreto 2693 de 2012 los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia y expide el Manual 3.1 de Gobierno en línea, como herramienta de autoayuda, que determina los lineamientos que deben seguir las entidades públicas y los particulares que desempeñan funciones administrativas en la implementación de la Estrategia en Colombia.[15]

2.4 SIEM (SECURITY INFORMATION EVENT MANAGER)

La gestión de logs se vale de la información enviada a la herramienta de recolección, lo que genera una gran responsabilidad al momento de seleccionar los dispositivos que se van a monitorear.[16]

Generar un equilibrio entre los diferentes dispositivos garantiza que se pueda obtener una información recolectada de forma organizada y permita su administración, sin importar el sistema operativo o el tipo de equipo.

---

[14] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Dirección de gobierno en línea. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: :http:// programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/ manual3.1.

[15] Ibíd.

[16]SOLARWINDS. SIEM, Seguridad de la información. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.solarwinds.com/siem-security-information-event-management-software.aspx

2.5 LEM (LOG EVENT MANAGER)

LEM como su nombre lo indica, es un administrador de eventos que se caracteriza por su alta capacidad en la gestión de logs y eventos, así como su facilidad en la implementación.[17]

Esta herramienta combina el análisis de los logs con la correlación de eventos, ofreciendo un control efectivo y confiable. Cuenta con un buscador avanzado que permite visualizar en tiempo real el desempeño, así mismo con su capacidad de administración robusta facilita a la entidad dar cumplimiento a las normatividades y mitigar las amenazas informáticas.

En resumen las principales características de estas herramientas son: combinar, registrar, gestionar logs de información, correlacionar la información en tiempo real, supervisar la integridad de archivos, permitir la búsqueda avanzada, así como su facilidad en la implementación.

2.6 SGSI (SISTEMA DE GESTIÓN DE SEGURIDAD EN INFORMACIÓN)

Se refiere a un conjunto de políticas de administración de la información, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la misma. Entendiéndose como integridad la completitud y exactitud de la información, confiabilidad a la disposición de la data y disponibilidad el acceso y uso de la misma.

El SGSI es el principal concepto en el que se basa ISO 27001, modelo construido para garantizar la buena práctica de la seguridad informática. La norma indica que el proceso de gestión de la seguridad de la información debe ser sistemático, además debe estar documentado, así como conocido por toda la entidad. [18]

Implementar un SGSI contribuye a la protección de la información vulnerable que manejan las entidades del estado y hace parte de la mitigación de riesgos o amenazas.

---

[17] SOLARWINDS. LOG & EVENT MANAGER, Eventos. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.solarwinds.com/log-event-manager.aspx

[18] ISO 27000.es. ¿Que es un SGSI?. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.iso27000.es/sgsi.html

2.7 ITIL

ITIL comprende cuatro elementos que garantizan el ciclo de vida del servicio: estrategia, diseño, transición y operación.

En la década del 1980 se crea un modelo para la prestación de servicios orientados a tecnología de la información que pueden ser aplicados a cualquier organización fomentando la implementación de mejores prácticas en las entidades que presten servicios de TI.

2.8 SEGURIDAD EN REDES

Se entiende por seguridad de redes, a la protección ejercida para evitar a los intrusos no autorizados, que puedan causar daños a los elementos de comunicación de la entidad.

El control lleva consigo mismo el monitoreo constante en cada uno de los equipos de la red, por ende la importancia de analizar los informes arrojados. No obstante, en la etapa inicial de implementación de la red se debe realizar la configuración de vlans para segmentar la red, con el fin de dificultar los ataques. Es una buena práctica separar las vlan por áreas de trabajo o importancia en la entidad.

Los dispositivos de red se deben configurar con un mínimo de parámetros que no permitan el acceso a personas no autorizadas, como puede ser usuarios limitados y contraseñas con características específicas.

2.9 HOST, NODOS Y DISPOSITIVOS DE RED

La red está conformada por host y nodos, que pueden ser hardware o software como switch, computadores, router, que permiten optimizar las conexiones. Los elementos anteriormente nombrados tienen una dirección MAC (Media Access Control), conocida como la dirección física, la cual es única para cada equipo.

2.9.1 Switch. Conocido en español como conmutador, este dispositivo permite la conexión e interacción de los equipos de la red, su función principal es interconectar dos (2) o más equipos de la red permitiendo el paso de datos de un dispositivo a otro. En el mercado se reconocen dos métodos de segmentación por los que separan los conmutadores que son de Switch capa 2 y Switch de capa 3, así como

la distribución de estos en la red también genera una diferencia entre estos por lo que se encuentra los Switch de Core y Switch de borde.

2.9.1.1 Switch capa 2. Su principal función es dividir la red en los múltiples dominios de colisión o segmentar la LAN, proceso que realiza mediante el análisis de la MAC destino del paqueteo trama. Switch capa 3 Además de las funciones del capa 2 permiten enrutamiento, validación del cableado, y soportan protocolos de enrutamiento (OSPF, RIP, etc.), redes virtuales y son recomendados para la segmentación de redes LAN

2.9.1.2 Switch de Core. Se atribuye esta característica al enrutador que se conecta con los dispositivos principales de la red como lo son los servidores firewall y routers, son dispositivos de alta velocidad al backbone, puertos WAN y se comporta como el cerebro de una red.

2.9.1.3 Switch de borde. Permiten la conexión del Switch de Core o los dispositivos de la red con los host o usuarios finales y work stations, sus propósitos finales son permitir y garantizar el acceso a la red.

2.9.2 Routers. Dispositivo de red conocido como enrutador que implementa una o más configuraciones para determinar la trayectoria del tráfico de la red, su función principal consiste en enviar paquetes de datos de una red a otra o interconexión de redes, parte de sus funciones es segmentar los paquetes para permitir la interconexión de redes que tengan tráficos de paquetes de diferentes tamaños.

2.9.3 Host. Cualquier dispositivo de la red que utilice TCP/IP. Un host es también un equipo en internet en el que se puede iniciar una sesión. Se puede usar FTP para conseguir archivos de una computadora host y usar otros protocolos (como Telnet).[19]

2.10 SERVIDORES

Cada uno de estos dispositivos reporta de forma independiente el comportamiento físico y lógico, lo que se conoce como evento o log y estos son motivo de verificación por el grupo de seguridad para minimizar riesgos de seguridad o normalizar el comportamiento de los mismos.

[19] RUSSEL, Charlie; CRAWFORD, Sharon; GEREND, Jason. Guía completa de Microsoft Windows Server 2003 Running+.España: Mc Graw Hill, 2003. p. 171-172.

2.10.1 Servidor de domino. Este servidor contiene las credenciales de todos los usuarios de la entidad, así como las diferentes políticas de acceso de los usuarios. Es el responsable de permitir o denegar mediante una autenticación el acceso al usuario a los dispositivos asignados y los elementos de red que a este se le otorgue acceso. Esta autenticación sea fallida o certera genera logs que son enviados al LEM.

2.10.2 Servidor de DHCP. Dispositivo de red que implementa el protocolo de configuración dinámica de host. Permite a los usuarios de la red obtener una dirección IP automáticamente conforme se van conectando a la red, esto se realiza de forma aleatoria y por el tiempo determinado por el administrador quien configura los rangos de direcciones y otros parámetros de red.

2.10.3 Servidor de correo. Dispositivo de red que mediante el uso de software especializado permite la distribución de correo electrónico mediante protocolos estándar, para esta labor algunos de los más conocidos son POP3 (puertos110 y 995), SMTP (puertos 25, 587,465) IMAP (puerto 143).

2.10.4 Servidores de aplicaciones. Dispositivo que provee uno o varios servicios de aplicaciones a los host de los usuarios que pertenecen a la red, sus principales características son la administración centralizada de las aplicaciones de la entidad. Las aplicaciones pueden estar alojadas y administradas desde uno más servidores dependiendo de su tamaño y prioridad.

2.10.5 Servidor de archivos. Dispositivo de red que contiene en un repositorio de todos los documentos de la entidad de forma centralizada lo que permite al administrador un mayor control sobre los documentos y su administración. Contiene los archivos de todos los usuarios registrados y con permisos de acceso, permite generar políticas para la administración de los archivos por parte de los usuarios finales así como el administrador.

2.10.6 Servidor de bases de datos. Dispositivos de red especializados en la gestión de grandes volúmenes de información, garantizando el acceso simultaneo de usuarios. Suministra servicios de almacenamiento, procesamiento, distribución y protección de datos.

2.10.7 Servidor web. Dispositivo de la infraestructura de red encargado de proveer y publicar servicios y contenidos desde redes externas a la entidad mediante el uso de puertos determinados (80, 8080, 443) y leguajes de programación estandarizados (HTML, PHP, .NET, Java, entre otros)[20]que permiten la visualización de los contenidos de una forma amigable para los usuarios finales.

---

[20] FORD, Verilee. Tecnologías de interconectividad en redes. México: Prentice-Hall.. 1998. P..645

2.11 DISPOSITIVOS DE SEGURIDAD PERIMETRAL

Elementos lógicos o físicos que se instalan y configuran en la red de la entidad con el propósito principal de prevenir y mitigar de manera significativa los riesgos que presenta los activos de la entidad, como lo son ataques de denegación, robo o fuga de información, accesos no autorizados, entre otros.

2.11.1 Firewall. Traducido al español es cortafuegos y la función principal es autorizar o restringir el paso a los equipos. El firewall puede ser un hardware o software diferente al antivirus, pero que de igual manera colabora con la protección, dado que impide que la red pueda ser atacada por hackers o software malicioso.

La protección y custodia de la información que este ejerce, es conformado por un patrón de seguridad entre la red interna y el internet, a su vez monitorea y analiza el acceso a los servicios.

Está diseñado y configurado principalmente para crear políticas de acceso, permitir o negar servicios, sin embargo, también es utilizado para limitar y monitorear el tráfico entre los diferentes ambientes en una red.[21]

2.11.2 Antivirus. Mecanismo implementado para analizar constantemente en los dispositivos de la red, como la memoria de un dispositivo, dispositivos de almacenamiento externo, conexiones a internet, navegadores web, descarga de archivos, en búsqueda de archivos malignos. Mediante la comparación de los archivos con bases de datos de resgistros conocidos como malignos (firmas de virus conocidas), el administrador de este software configura las acciones a tomar.

La Real Academia Española (RAE) define antivirus como: dicho de un programa que detecta la presencia de virus y puede neutralizar sus efectos.[22]

2.11.3 IDS. Sistema de detección de intrusos, puede estar conformado por un mecanismo físico (hardware) o lógico (software), el cual realiza un monitoreo constante de la red interna con el fin de detectar ataques a los dispositivos conectados a la red.

2.11.4 IPS. Sistema de prevención de intrusos mediante el análisis de tráfico entrante a la red interna de la entidad, valida o niega el acceso a los paquetes de datos, lo que permite tomar acciones como bloqueo, eliminación y cuarentena de

---

[21]WINDOWS. MICROSOFT. ¿Que es un firewall?. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://windows.microsoft.com/es-co/windows/what-is-firewall#1TC=windows-

[22]RAE. Real Academia Española. ¿Qué es antivirus? [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://lema.rae.es/desen/?key=antivirus

los paquetes. El administrador del dispositivo es quien configura los parámetros de detección así como las acciones a tomar con los paquetes detectados como maliciosos.

2.11.5 DLP. Acrónimo para *Data Loss Prevention*, hace referencia a los sistemas que identifican, monitorean y protegen los datos por medio de una inspección profunda de contenido y análisis de transacciones, con el objetivo de detectar y evitar el uso no autorizado de la información.

2.11.6 Email Gateway. Dispositivo físico o virtual configurado en la red de la entidad para monitorear y analizar todo el tráfico de correo que entra y sale de la ANSPE, basada en la parametrización de reglas y políticas que permiten recibir, enviar, denegar, bloquear o poner en cuarentena los correos de la misma. Su base de datos se actualiza diariamente con el proveedor que para el caso es McAffe, permite el bloquear y reportar correos SPAM o con malware lo que previene desarrollo de ataque por parte de correo electrónico.[23]

2.11.7 Web Gateway. Dispositivo físico configurado en la red de la entidad para realizar detección de amenazas Web y malware, mediante el análisis de todo el contenido de las páginas web que se consultan desde la red de la entidad, lo que proporciona una capa de seguridad inmediata, detectando amenazas o ataques de día cero, spyware y dirigidos sin firma.[24]

2.12 PROTECCIÓN DE DATOS Y POLÍTICAS DE SEGURIDAD

La implementación de políticas de seguridad y protección de datos se ejecutan en cada entidad para custodiar los activos de la información, con el fin de que esta sea revelada o modificada únicamente por el usuario autorizado. De igual manera la entidad en el proceso de diseño de las políticas debe ser estricto con el manejo de confiabilidad para todas las personas que intervenga en el tratamiento y uso de la información.

Lo que lleva a que se conserve los tres fundamentos disponibilidad, integridad y confidencialidad. Para esto es indispensable que previamente se realice el inventario de los dispositivos con los que cuenta la entidad, sus activos e identificar sus vulnerabilidades, así determinar en donde se debe centrar la protección.

---

[23] MCAFEE. Email Gateway. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.mcafee.com/us/products/email-gateway.aspx

[24] MCAFEE. Web Gateway. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.mcafee.com/us/products/web-gateway.aspx

Posterior de la identificación de las vulnerabilidades, se deben diseñar los lineamientos que contribuyan a la mitigación de los riesgos, lo que se denomina políticas de seguridad.

3. MODELO DE INVESTIGACIÓN

3.1 ACOMPAÑAMIENTO Y ASESORAMIENTO

Este proyecto se desarrolla usando estudios de especialistas en buenas prácticas de almacenamiento, gestión y análisis de log, así como en la experiencia de la instalación y gestión de log, lo que permite una adecuada detección de incidentes de seguridad.

3.2 ENFOQUE DE LA INVESTIGACIÓN

Un enfoque permite integrar los conceptos de la seguridad con teorías de soluciones e implementación de herramientas de seguridad aplicada a normas y estándares conocidos. Dado que involucra los controles de una norma y gestiona la solución para que esta se cumpla y mitigue los riesgos.

3.3 COMPLEJIDAD

Los principales limitantes en la implementación son los presupuestos y costos que puede generar esta herramienta, dado que no solo son los costos de equipos si no el tiempo del administrador, las horas de configuración y afinamiento de la herramienta. Motivo por el cual se debe tener en cuenta lo explicado…véase el numeral 6.1… referente a los recursos y requisitos a cumplir como un sistema SGSI implementado.

4. METODOLOGÍA DE IMPLEMENTACIÓN

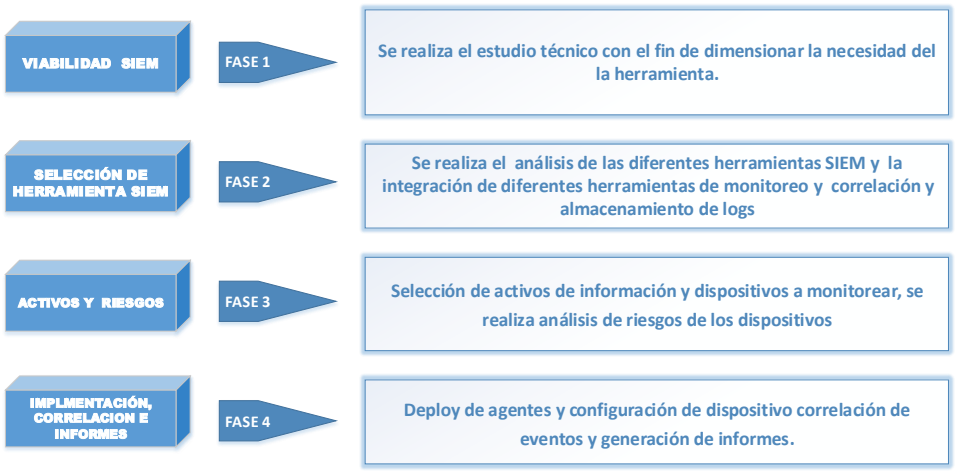
La implementación de una herramienta SIEM debe realizarse por etapas o fases que ayuden a una correcta configuración y análisis de los eventos o logs recolectados, de esta manera realizar un análisis de los equipos más relevantes que conforman la infraestructura de la entidad, con el fin de que envíen la información parametrizada a las herramientas SIEM.

Las herramientas SIEM basan su correcto funcionamiento en un proceso adecuado de selección de los dispositivos en la infraestructura de la entidad, con el fin de obtener los datos para realizar el respectivo análisis y monitoreo de los mismos. Es significativo normalizar este procedimiento para estandarizar la información de los eventos que estos generan, sin importar el sistema operativo o la aplicación que estos desarrollan en la entidad.

Una buena administración de eventos de seguridad optimiza la auditoría a los eventos que son recolectados, almacenados y que deben estar disponibles facilitando el cumplimiento de políticas de seguridad y previniendo fallas técnicas o fugas de información.

La implementación de la herramienta basada en la metodología de fases permite realizar un análisis correcto de los dispositivos a monitorear, fundamentado en la prioridad y el valor de cada uno de los dispositivos de la entidad, aspectos que son identificados con la ayuda de un SGSI y el inventario de activos. La descripción de las fases de implementación SIEM se puede visualizar en la Figura 1.

Figura 1. Fases de implementación SIEM



Fuente autor

4.1 PRESUPUESTO

En la estimación del presupuesto, se debe tener en cuenta el costo de los recursos humanos adicional a la adquisición de los recursos técnicos.

4.1.1 Recurso técnico. El presupuesto técnico esta dado en dólares, por lo que al realizar un presupuesto en la moneda Colombiana se debe tener presente el T.R.M. En el Cuadro 1 se puede visualizar la cantidad y el valor de cada uno de los elementos técnicos requeridos.

Cuadro 1. Presupuesto técnico

Descripción	Cantidad	Valor Unitario ($)	Valor Total ($)
Licenciamiento	1	5.000	5.000
Horas adecuación server	10	50	500
Horas consultoría	50	100	5.000
Total			**10.500**
Fuente autor			

4.1.2 Recurso humano. El recurso humano es un costo que debe ser estimado e incluido dentro del presupuesto para adquirir la herramienta. Por lo anterior en la Cuadro 2 se observa cada una de las actividades y recursos requeridos.

Cuadro 2. Actividades y costos

Actividad	Recursos	Horas	Costo (Pesos)	Total (Pesos)
Levantamiento de información	2	40	35.000	1.400.000
Analizar información	2	40	35.000	1.400.000
Consolidar información	2	40	35.000	1.400.000
Validación Activos	1	80	35.000	2.800.000
Solicitud servidor	1	40	35.000	1.400.000
Diseño plan trabajo	1	40	35.000	1.400.000
Presentación a la entidad	1	40	35.000	1.400.000
Despliegue de agentes	1	120	35.000	4.200.000
Monitoreo de implementación	1	40	35.000	1.400.000
Auditoria	1	40	35.000	1.400.000
Total		520		18.200.000
Fuente autor				

4.2 PROGRAMACIÓN SEMANAL DE ACTIVIDADES

El cuadro 3 plantea las actividades generales y específicas para la asignación de recursos.

Cuadro 3. Programación de actividades

TIEMPO	ACTIVIDAD	ACTIVIDADES ESPECÍFICAS
Semana 1	Levantamiento de Información	Seguridad informática en Colombia
		Gobierno en línea
		Herramientas SIEM
Semana 2	Analizar la Información	Estructurar la información basado en las necesidades de la entidad
Semana 3	Consolidar Información	Depurar información
Semana 4		Validar la información necesaria
Semana 5	Validar Activos de la Entidad	Inventario de activos
Semana 6	Validar Activos de la Entidad	Selección de activos
Semana 7	Solicitar Servidor	Validar requerimientos mínimos para implementación de herramienta
Semana 8	Diseño del Plan de Trabajo e Implementación	Definir orden y cronograma de despliegue de agentes
Semana 9	Presentación RFC en la Entidad	Presentación en control de cambios
		Análisis y puesta en marcha
Semana 10	Despliegue de Agentes	Validación de impacto en el servidor
Semana 11		Captura de logs
Semana 12		análisis de impacto
Semana 13	Monitoreo de Implementación	Validación de estado de logs y cantidad
Semana 14	Auditoria	Control de log monitoreados y validación de su operación
Fuente autor		

4.3 PERIODO DE IMPLEMENTACIÓN

El tiempo estimado para la implementación son catorce (14) semanas, en donde las actividades son seriales y no paralelas. El cuadro 4 evidencia que la duración de las actividades está dada en días laborales.

Cuadro 4. Programación de actividades

Nombre de tarea	Duración	Comienzo	Fin
Levantamiento de Información	5 días	lunes 01/09/14	Viernes 05/09/14
Analizar la Información	5 días	lunes 08/09/14	Viernes 12/09/14
Consolidar Información	5 días	lunes 15/09/14	Viernes 19/09/14
Validar Activos de la Entidad	10 días	lunes 22/09/14	Viernes 03/10/14
Solicitar Servidor	5 días	lunes 06/10/14	Viernes 10/10/14
Diseño del Plan de Trabajo e Implementación	5 días	lunes 13/10/14	Viernes 17/10/14
Presentación RFC en la Entidad	5 días	lunes 20/10/14	Viernes 24/10/14
Despliegue de Agentes	15 días	lunes 27/10/14	Viernes 14/11/14
Monitoreo de Implementación	5 días	lunes 17/11/14	Viernes 21/11/14
Auditoria	5 días	lunes 24/11/14	Viernes 28/11/14
Fuente autor			

4.4 FUNDAMENTOS DE HERRAMIENTAS SIEM

Con la creciente necesidad de analizar y crear reportes en tiempo real y de forma efectiva para los eventos que ocurren en las entidades, se desarrollan herramientas que permitan correlacionar las alertas generadas por los dispositivos de red, servidores, así como por las diferentes aplicaciones con las que cuenta la infraestructura de las entidades.

Las herramientas conocidas para llevar a cabo el proceso descrito anteriormente, reciben el nombre de SIEM y su correcto funcionamiento se basa en la administración y almacenamiento de Log que se registran en los diferentes dispositivos de la infraestructura y red de las entidades, el éxito de la gestión de estos logs se caracteriza por una adecuada selección de los dispositivos o activos a monitorear y analizar.

Dado que se tiene diferentes dispositivos a analizar, existe una diferencia en la información que se recibe de estos, por lo que es necesario realizar una normalización o estandarización de dicha información, para garantizar que sin importar el sistema operativo o tipo de dispositivo la información almacenada sea de fácil acceso y análisis, lo que permite una generación de reportes e informes de forma más rápida y eficiente.

4.4.1 Funcionamiento de una herramienta SIEM. Las Herramientas SIEM fundan su operación en 6 elementos que permiten el procesamiento y la gestión de logs de forma que facilite al administrador un eficiente análisis. Estos elementos pueden operar de manera independiente, sin embargo realizar el trabajo en conjunto optimiza la funcionalidad de los SIEM. Dichos elementos son: dispositivo de origen, colector de logs, normalización y filtrado de logs, almacenamiento de logs, motor de reglas, monitoreo análisis y recuperación de eventos.

4.4.2 Capas de los SIEM. Las herramientas SIEM cuentan con una serie de etapas, que definen un orden para desarrollar, implementar y configurar los diferentes dispositivos o elementos de infraestructura, que garantiza una correcta aplicación de la misma. Las cuatro capas se pueden observar en la Figura 2.

Figura 2. Capas de implementación SIEM

Fuente autor

La parametrización de las capas garantiza que la herramienta confiera su máxima capacidad de funcionamiento y entrega de informes.

4.5 SELECCIONAR UNA HERRAMIENTA SIEM

4.5.1 Comerciales más conocidos. El mercado ofrece varias soluciones que permiten la implementación de Herramientas SIEM, entre las cuales se destacan por sus marcas o empresas de desarrollo y el prestigio que tiene estos fabricantes.

4.5.1.1 SIEM – McAfee - NitroSecurity. La herramienta utiliza un motor de bases de datos para identificar, correlacionar y mitigar amenazas. Permite bajo una sola plataforma implementar la gestión de eventos y se destaca como una empresa líder en el desarrollo de soluciones SIEM. Puede establecer un conjunto de acciones de monitoreo, analizar log forenses, así como implementar políticas y deploy de actualizaciones, entre otras.[25]

La integración de las tecnologías SIEM de Nitro Security en la familia de productos McAfee permite a las empresas utilizar una única plataforma para el análisis y gestión de eventos, identificar rápidamente, correlacionar y remediar amenazas, mitigando los riesgos para la información y la infraestructura, analizar los datos de log y eventos forenses creados por redes, bases de datos y aplicaciones, instituir una gama de monitoreo y mitigación acciones, como la emisión de nuevas configuraciones, la aplicación de nuevas políticas y la implementación de actualizaciones de software.

4.5.1.2 SIEM – SolarWinds– LEM. Ofrece una arquitectura con la implementación de diferentes herramientas entre las cuales se destaca el analizador y correlacionado de eventos o LEM (*Log Evento Manager*), así como el Log Analizar Software que permite al administrador realizar un monitoreo de los eventos que se vinculen a la herramienta de forma sencilla y mediante una configuración amigable a través de la instalación de agentes de monitoreo. [26]

Las diferentes Herramientas de este fabricante que contemplan una solución SIEM para empresas de diferentes tamaños son*:* log & event manager, patch manager, firewall security manager y security managed file transfer server.

4.5.1.3 SIEM – HP – ArcSight ESM. Empresa líder en el mercado que ofrece un conjunto de soluciones para la implementación de una SIEM con variedad de

---

[25] MCAFEE. Nitro Security. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.mcafee.com/us/about/mcafee-nitrosecurity.aspx

[26] SOLARWINDS. LOG & EVENT MANAGER, Generalidades de la empresa. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.solarwinds.com/log-event-manager.aspx

productos para empresas de diferentes tamaños, en donde su producto principal es la herramienta ArcSight ESM, ya que permite la integración de los demás elementos y actúa como repositorio de logs e incluye paquetes de cumplimiento para las normas de seguridad más conocidas.[27]

Hewlett Packard realiza la compra en el 2010 de la compañía ArcSight y entre los productos que tienen el mercado se destacan: ArcSight ESM, ArcSight Managment Center, ArcSight Logger, ArcSight Aplication View, ArcSight Express, ArcSight Insight Packages y ArcSight Treat detector.

4.5.1.4 SIEM – IBM – Sequrity QRadar. Ofrece una arquitectura unificada en la que integra la gestión de sucesos e información de seguridad, la gestión de registros y anomalías, la gestión de la configuración y vulnerabilidades.[28]

Los productos que este fabricante ofrece son: una única arquitectura para analizar registros, flujos, vulnerabilidades, usuarios y datos de activos, detección de próximas anomalías en el comportamiento y correlación en tiempo real para identificar amenazas de alto riesgo, detección de incidentes de alta prioridad entre billones de puntos de datos, visibilidad completa de red, aplicaciones y actividades de usuario, conformidad regulatoria automatizada con funcionalidades de recopilación, correlación y creación de informes.

Los productos que ofrece para la implementación de la herramienta son: IBM Security QRadar Incident Forensics, IBM Security QRadar Log Manager, IBM Security QRadar QFlow Collector, IBM Security QRadar Risk Manager, IBM Security QRadar SIEM, IBM Security QRadar VFlow Collector y IBM Security QRadar Vulnerability Manager.

4.5.1.5 SIEM– EMC2 – RSA. Ofrece soluciones escalables a medida que los clientes van creciendo y configurando sus dispositivos, RSA pertenece a la empresa EMC2 en la división de seguridad. Está orientado a la seguridad de la información, a medida que la empresa cliente va evolucionando pueden encontrar herramientas que faciliten el cumplimiento de las necesidades.[29]

EMC2 bajo la plataforma RSA ofrece una gran cantidad de productos entre los cuales se encuentran los siguientes:

---

[27]HP. SIEM. ARCSight ESM. Solución de sogtware. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www8.hp.com/us/en/software-solutions/arcsight-esm-enterprise-security- management/index.html

[28]IBM. IBM QRadar Security Intelligence Platform. [en línea], [Consultado el 23 de Noviembre de2014]. Disponible en: http://www-03.ibm.com/software/products/es/qradar

[29]EMC2. RSA Security Analitics. [En linea]. [Septiembre 2014] Disponible en: http://colombia.emc.com/search.htm?fromGlobalSelector#search/query:q=SIEM;p:cPage=1

- RSA Access Manager
- RSA enVision
- RSA Adaptive Authentication
- RSA Archer Assessment and Authorization for Federal Government Agencies
- RSA Archer Audit Management
- RSA Archer Business Continuity Management
- RSA Archer Compliance Management
- RSA Archer Enterprise Management
- RSA Archer Incident Management
- RSA Archer Platform
- RSA Archer Policy Management
- RSA Archer Risk Management
- RSA Archer Security Operations Management
- RSA Archer Threat Management
- RSA Archer Vendor Management
- RSA Archer eGRC
- RSA Authentication Manager
- RSA BSAFE
- RSA Data Loss Prevention
- RSA Data Protection Manager
- RSA ECAT
- RSA Federated Identity Manager
- RSA Identity Protection and Verification
- RSA Identity and Access Management
- RSA NetWitness Broker

4.5.2 No comerciales conocidos. Son soluciones generalmente de código abierto que representa una alternativa para las empresas que desean implantar una solución de seguridad con bajo presupuesto o no han realizado el análisis y comparación de costo beneficio que ofrecen este tipo de herramientas.

4.5.2.1 Cyberoam iView. Elite Core Technologies Ltda. Realiza un proceso de mejoras y publicación a una herramienta de código abierto. OEM como es conocido cuenta con módulos de recopilación de logs, reportes, gestión de seguridad y análisis forense, de igual forma se puede obtener el software de código abierto y adaptarlo a las necesidades de la entidad.[30]

4.5.2.2 OSSIM. Desarrollado por la empresa Alien Vault, sus siglas indican Open Source Security Information Managment. La descarga es gratuita al ser código

[30] CYBEROAM. Intelligent Logging & Reporting. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.cyberoam-iview.org

abierto por lo que es necesario entender que presenta limitaciones de almacenamiento, desempeño y no cuenta con un soporte técnico.[31]

No obstante, presenta una plataforma que permite realizar pruebas para conocer los benéficos y desventajas de este producto lo que facilita a la entidad evaluar la necesidad de adquirir o no una herramienta SIEM.

Existe una versión paga que permite un mayor número de beneficios de la herramienta OSSIM, lo que facilita implementar una herramienta de bajo costo y de marcas no reconocidas.

4.6 CONFIGURAR LOS COMPONENTES DEL SIEM

Las herramientas SIEM se desarrollaron tras la necesidad de analizar de forma rápida y eficiente los eventos que ocurren en los dispositivos de red, servicios y aplicaciones, junto con ello nace la posibilidad de realizar reportes y prevenir fallas o pérdidas de información y servicios.

Teniendo en cuenta lo anterior y de acuerdo a la solución requerida, se debe realizar la selección de la herramienta con la cual se va a trabajar y por ende analizar las prestaciones que esta tiene.Para el caso de la herramienta seleccionada en este proyecto, la cual corresponde a LEM de SolarWinds está compuesta por 6 capas definidas de acuerdo a como se observa en la Figura 3:

Figura 3. Elementos de herramienta SIEM

Fuente autor

[31] ALIENVAULT. The World´s Most Widely Used Open Source SIEM [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: https://www.alienvault.com/open-threat-exchange/projects

4.6.1 Dispositivo de origen. Se puede definir como dispositivo de origen cualquier equipo de red, de servicios o de almacenamiento que genere registros que se quieran analizar en el SIEM, es decir la fuente de información de la herramienta.

Este dispositivo se debe seleccionar basado en la importancia para la entidad y la necesidad de monitorear su comportamiento, teniendo en cuenta que no es requerido analizar todos los eventos que genere. Otro aspecto a considerar para la selección de los dispositivos de origen, es analizar los activos críticos y las vulnerabilidades de la entidad.

4.6.2 Colector de logs. La función de un colector debe ser un proceso automático que permita obtener los datos de los eventos.[32]

La recolección de datos se puede realizar de dos formas, una de ellas es enviar los logs desde el dispositivo origen a la herramienta SIEM mediante SYSLOG o SNMP configurando la IP, puerto y nombre del DNS de la herramienta SIEM para él envió de los datos. Otra forma de recolección de datos es realizar una conexión con el dispositivo de origen, leyendo archivos en los que se almacena los registros de las aplicaciones, para el caso de bases de datos se puede realizar mediante el protocolo ODBC lo que permite traer los registros.

La herramienta LEM de SolarWinds implementa la recolección de datos mediante la instalación de agentes en los dispositivos, si el sistema operativo lo permite, de otra forma se envían los registros SYSLOG al SIEM para que este pueda almacenarlos y posteriormente ser analizados.

4.6.3 Normalización y filtrado de logs. Los dispositivos de origen envían registros constantemente, lo que requiere un filtrado que evalué el tipo de dato requerido y así evitar la saturación de eventos en la herramienta

Los datos que mayor importancia representan para los dispositivos de origen generalmente son los logs de Warning o Error y los que menos importancia representa son los logs de transacciones a no ser que sea necesario el monitoreo de las mismas.

Para el análisis de los logs también se pueden utilizar categorías de seguridad, cambios de configuración, auditorias, acceso y permisos en archivos, ataques de tipo overflow, denegación de servicios, etc.

---

[32] SWIFT David, A practical Application of SIM/SEM/SIEM Automating Threat Identification. SANS USA: Institute Infosec Reading Room, 2007 p.19.

4.6.4 Almacenamiento de logs. Es necesario contar con un mecanismo de almacenamiento de Logs para optimizar los procesos, por ende se requiere una base de datos robusta que permita analizar el histórico de los eventos y así generar los informes y reportes.

De aquí que la infraestructura debe contar con unos requerimientos mínimos, con el propósito de ejecutar el análisis y búsqueda en la herramienta, por ejemplo para el caso de la última versión de LEM del fabricante SolarWinds es necesario un servidor Windows 8 R2 con 8 GB de memoria Ram como mínimo.

4.6.5 Motor de reglas. Esta capa de correlación de logs permite construir las reglas y alertas en la Herramienta SIEM, en donde la complejidad o sencillez depende del método utilizado y la cantidad de información a correlacionar. El motor de reglas se basa en una lógica booleana para determinar si un evento reúne los parámetros especificados.

Cuando se desea conocer si un archivo fue eliminado de un servidor cualquiera por un usuario no autorizado, se puede hablar de un ejemplo claro de una regla.

4.6.6 Monitoreo y reportes. La última capa de una herramienta SIEM permite la interacción y uso de los logs almacenados, de tal manera que se pueda analizar eficientemente la información, con el fin de generar reportes y alarmas.

Las Herramientas SIEM cuentan con una interface de administración para los usuarios que hace más amigable la interacción con los logs almacenados, permitiendo de una forma sencilla la correlación de eventos, programación de tareas y prevención de ataques o fallas en los dispositivos.

4.7 NORMA ISO 27000

Las normas ISO 27000 son un elemento útil al momento de configurar la herramienta SIEM para optimizar la generación de reportes e información que se desea adquirir de la misma. Así mismo, facilitan al administrador auditar el comportamiento de los dispositivos, encontrar posibles anomalías y almacenar la evidencia para futuras consultas.

4.7.1 ISO 27002-2005. El proceso de implementación de un SGSI es acompañado de la norma ISO -27002, en el cual se encuentran 11 lineamientos que permiten establecer procedimientos para mantener y mejorar el SGSI. Un mínimo de requerimientos con los que aporta la Herramienta SIEM a la Implantación de SGSI con base en la norma ISO 27002-5 es en la caracterización y cumplimiento de los controles descritos y que se toman como guía mínima:

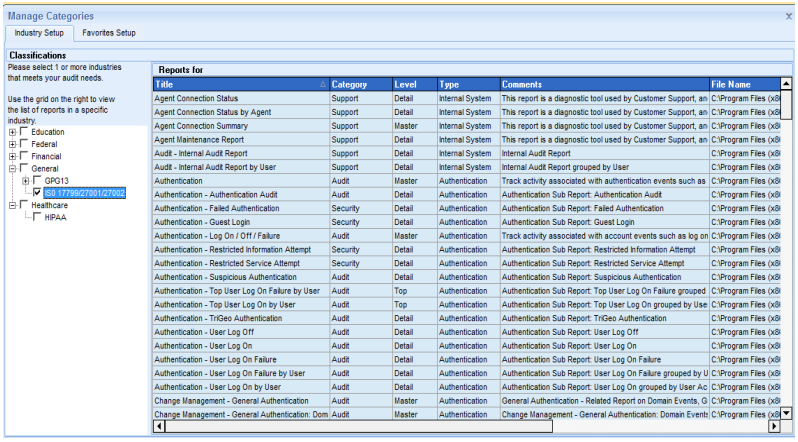
4.7.1.1 Herramienta SIEM RSA. Del fabricante EMC2 en los reportes que genera de forma predeterminada se puede evidenciar diversos controles referenciados en la norma, como muestra la Figura 4:

Figura 4. RSA en Visio EMC2 [33]

Fuente Página web Colombia.emc

4.7.1.2 Herramienta SIEM LEM del fabricante SolarWinds. Como parte de sus reportes preconfigurados cuenta con informes específicos para la norma ISO27000. En la Figura 5, se evidencia la interface gráfica de *Reporter* de la herramienta LEM.

Figura 5. Imagen herramienta Reporter LEM



Fuente Software LEM

[33] SIMPLIFIED IT COMPLIANCE. ISO 27002-based Compliance Frameworks RSA Solutions. [En linea]. [Octubre 2 de 2014]. Disponible en: http://colombia.emc.com/collateral/microsites/ forum 2008/forum2008-security-simplified-it-compliance.pdf

4.8 INCIDENTES DE SEGURIDAD

Son todos los eventos desfavorables que se generan en un entorno informático y a su vez comprometen los 3 pilares de la información CID (Confidencialidad, Integridad y Disponibilidad).

Los reportes que generan los diferentes dispositivos son el recurso principal para una herramienta SIEM, dado que permiten identificar de manera inmediata los eventos presentados y el histórico. De esta manera el oficial de seguridad o quien este designado actuará proactivamente.

4.8.1 Evento o incidente. Es toda evidencia observable en un entorno informático, cualquier acontecimiento que se pueda identificar y afecte la operación normal de la red, el sistema y sus aplicaciones. Estos pueden ser frecuentes o esporádicos, sin embargo para todos se debe identificar la información que contiene cada uno de estos.

4.8.2 Gestión de incidentes. El manejo de incidentes de forma inmediata o la prevención de los mismos, debe ser una de las caracterizas a tener en cuenta al momento de adquirir o pensar en la implementación de una herramienta SIEM, así como en la implementación de la infraestructura para contar con la capacidad de almacenamiento y procesamiento requeridos en la entidad.

4.9 IMPLEMENTACIÓN DE HERRAMIENTA SIEM SIN SGSI

La ausencia de un SGSI no es un impedimento para la implementación de una herramienta SIEM. Para esto la entidad debe apoyarse de los estándares establecidos e identificar los activos que considera se deben monitorear.[34]

Es por lo anterior que una de las características más importantes, es la definición de los activos de información críticos para la entidad, con los cuales se crea las condiciones y necesidades para garantizar la seguridad, integridad y disponibilidad de la información. Otro aspecto relevante es realizar un análisis de vulnerabilidades a estos activos previamente definidos, lo que permite implementar de forma adecuada la seguridad perimetral con los que cuenta la entidad. Paralelamente se

[34]ARIAS, Luis. COGOLLO, Jhony. Procedimiento para la implementación de una Herramienta SIEM en empresas que cuenten con un sistema de gestión de seguridad de la información. Bogotá. Trabajo de grado. Universidad Piloto de Colombia. Especialización en Seguridad informática. 2013. pag 43.

debe realiza el análisis y diseño del plan de remediación para cada una de las vulnerabilidades identificadas garantizando la continuidad del negocio.
El equipamiento necesario para realizar una protección de la información con dispositivos de seguridad se plantea posterior a la definición de los activos con sus vulnerabilidades y medios de remediación, dado a que de ellos se obtiene parte de la información que será correlacionada en las herramientas SIEM.

No contar con un SGSI obliga a que se definan responsables y funciones, para la atención de incidentes, requerimientos, así como los procesos que se van a ejecutar o los niveles de escalamiento que se deben tener para gestionar los eventos o sucesos que se presenten.

El oficial de seguridad persona encargada de liderar el proceso de implementación, debe definir las tareas específicas de los administradores de dispositivos y servicios, lo cual le permitirá optimizar los tiempos de respuesta, obtener informes funcionales y mantener un constante monitoreo y mejoramiento de la herramienta, adicional la responsabilidad es compartida lo que mitiga el riesgo de errores, agiliza el tiempo de respuesta y optimiza la configuración.

4.10 IMPLEMENTACIÓN DE HERRAMIENTA SIEM CON SGSI

Con el sistema de Gestión de Seguridad de la información, se facilita implementar la herramienta SIEM, dado que se atienden los lineamientos definidos por parte de la dirección de la entidad y el oficial de seguridad, responsabilizando los diferentes actores que interactúan con los dispositivos de la red y activos de información. De igual manera se garantiza el conocimiento de la entidad frente al valor de la información y la necesidad de gestionar los recursos necesarios para proteger de forma óptima los activos.[35]

Contar con un SGSI indica que la entidad es consciente de la importancia de los activos de información para la continuidad del negocio y basado en esto se han desarrollado una serie de pasos y procedimientos sustentados en diferentes documentos que permiten mitigar los riesgos y mantener la continuidad de los servicios.

Una de las normas más implementadas por el gobierno Colombiano, a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), para la construcción y como apoyo al SGSI es la norma ISO 27000 entre la que se

[35] Ibíd., p. 43.

encuentra los estándares asociados a la seguridad de la información. En la Tabla 1 se puede evidenciar los principales estándares que constituyen la norma.

Tabla 1. Norma ISO 27000

Norma ISO 27000
ISO 27000 Fundamentos y vocabulario
ISO 27001 Requerimientos de un SGSI
ISO27002 Código de buenas practicas
ISO 27003 Guía de implantación
ISO 27004 Métricas e Indicadores
ISO 27005 Guía para el Análisis y Gestión del Riesgo
ISO 27006 Especificaciones para organismos certificadores
ISO 27007 Guía de requisitos para entidades auditoría y certificación

Fuente Norma ISO 27000

5. IMPLEMENTACIÓN DE SIEM EN ANSPE

A la fecha de construcción de este documento, la ANSPE se encuentra en la fase de planear del SGSI, motivo por el cual se plantean dos posibles proceso de implementación de la herramienta SIEM, con el fin de avanzar en la seguridad de los dispositivos. El primer escenario que atiende la necesidad de la entidad es realizar un proceso de selección de activos basado en la importancia que se le da a los dispositivos y a la información por parte del área de tecnología y el segundo escenario es implementar la selección de dispositivos a monitorear basado en el levantamiento de activos que realiza el oficial de seguridad de la entidad.

Es de aclarar que lo anterior no es condicionante para iniciar el proceso de implementación de una solución SIEM en la entidad, no obstante si son alternativas en el momento de la definición de activos a monitorear, dado que no se cuenta con un SGSI finalizado.

Luego de estudiar los fundamentos y características de una herramienta SIEM y conociendo las necesidades de la ANSPE se toma la decisión de implementar el dispositivo LEM de SolarWinds como herramienta de recolección análisis y consulta de log.

Teniendo claridad de lo que ofrece la herramienta seleccionada se determina que en la fase inicial la Herramienta SIEM se va a proceder con los avances del SGSI que se tienen a la fecha, validando previamente los dispositivos a monitorear con ayuda del jefe de la oficina de tecnologías y el oficial de seguridad.

Con lo anterior se realiza un análisis y levantamiento de información de activos que permite avanzar en la implementación del SGSI y un futuro fortalecimiento de la herramienta SIEM.

5.1 FASE 1 VIABILIDAD

El tamaño de la entidad y el proceso de implantación del SGSI, así como la de los modelos de seguridad y gobierno en línea son factores que se deben tener en cuenta a la hora de estimar el recurso económico y personal para implementar la herramienta.

Al contar con la Herramienta LEM de SolarWinds y con la etapa inicial del SGSI se debe proceder a la implementación con los mínimos requerimientos e ir realizando avances periódicos, con el fin de implementar una solución SIEM que cumplan con

las necesidades de la entidad, las cuales se ajustaran a medida que se implemente la solución SGSI.

Con la herramienta disponible se pueden realizar avances que permitan acompañar la implantación de la fase planear de SGSI para la entidad.

5.2 FASE 2 SELECCIÓN HERRAMIENTA

La ANSPE cuenta con un herramienta de monitoreo, correlación y almacenamiento de logs del fabricante SolarWinds que permite llevar a cabo una implementación inicial de una herramienta SIEM. Para el caso específico esta herramienta es un administrador de log y eventos o LEM por sus siglas en ingles.

Una descripción de la implementación de la herramienta se puede observar…en el ANEXO A…, así como de la activación de su licencia y requerimientos mínimos para su configuración sin contar con un SGSI, de forma tal que seleccionen los dispositivos críticos de la entidad y se realice un monitoreo de los mismos.

5.3 FASE 3 ACTIVOS Y RIESGOS

Parte del avance que se tiene el SGSI permite identificar los activos principales de la entidad, entre los cuales se encuentra dispositivos de red, de seguridad, de almacenamiento, servidores y dispositivos de seguridad perimetral.

Igualmente se debe realizar el levantamiento de activos y analizar sus vulnerabilidades para identificar la importancia y criticidad, con el fin de obtener una valoración de estos y con esto realizar la implementación de la herramienta. Para cada uno de los activos se debe identificar un gestor o administrador.

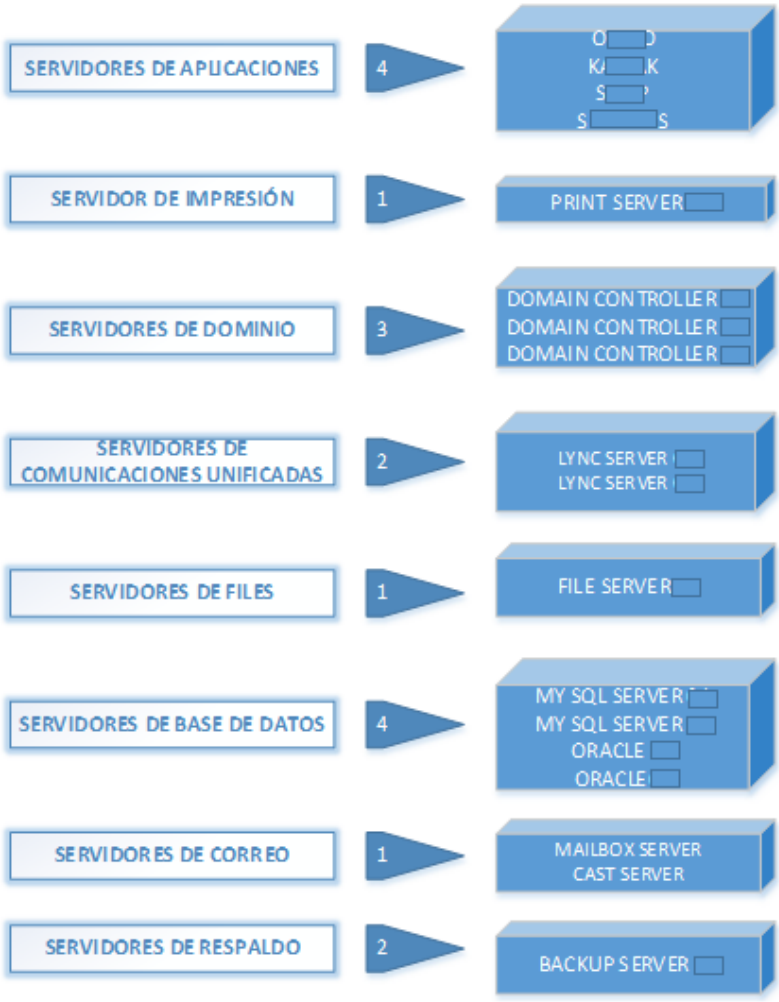
Posterior a ello se debe realizar un proceso de despliegue de agentes en los diferentes activos de información, este proceso se describe de forma general para los dispositivos,…ver el ANEXO B…en el cual se ilustra la instalación para los diferentes sistemas operativos.

Es de anotar que la herramienta LEM adquirida cuenta con un software de licenciamiento anual para el monitoreo de 30 dispositivos a través de agentes o conectores.

Para conocer con mayor detalle las diferentes etapas del proceso, a continuación se describen cada una.

5.3.1 Identificar los activos. Al identificar los servidores principales se encuentra los controladores de dominio, servidores de aplicaciones, almacenamiento, correo, comunicaciones, impresión entre otros. Los activos priorizados en la entidad se observan en la Figura 6 la cual se muestra a continuación:

Figura 6. Activos priorizados ANSPE

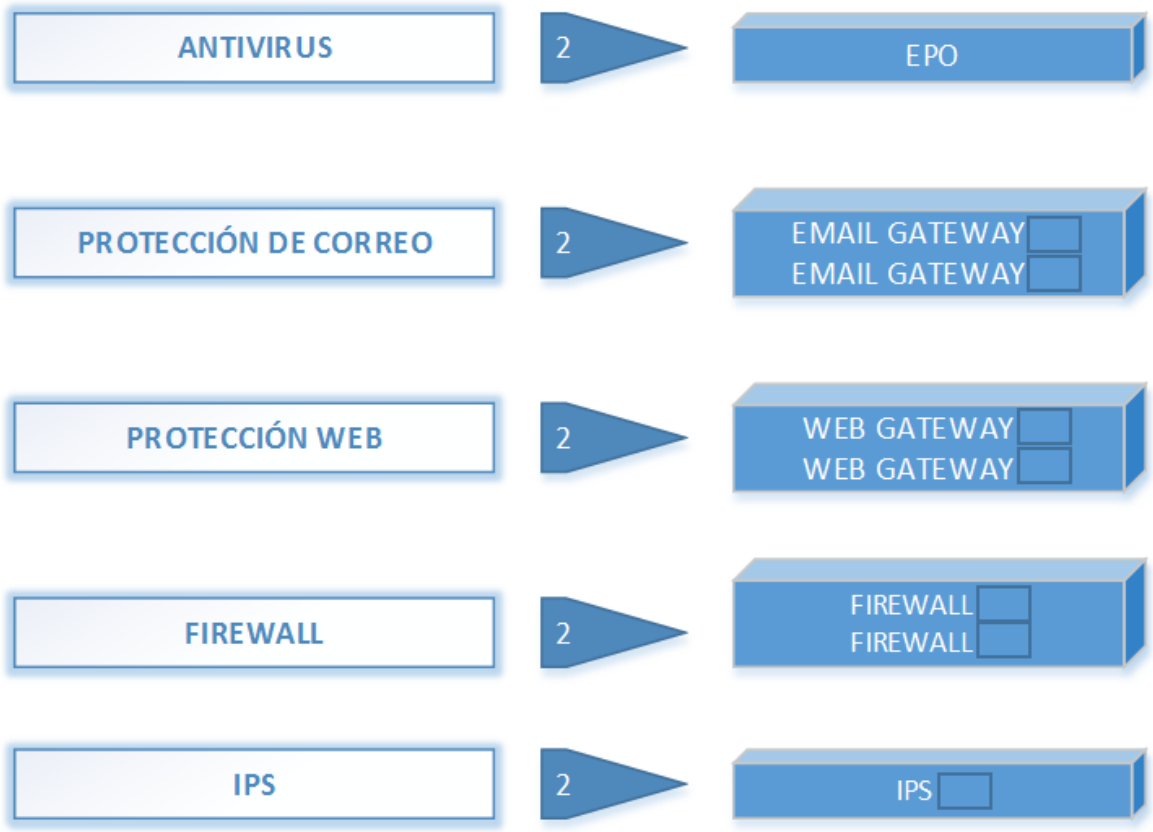


Fuente autor

Se obtiene un total de 18 dispositivos en los cuales se instalará el agente de LEM para su monitoreo y correlación de Log.

Luego de seleccionados los servidores se procede a analizar los dispositivos de seguridad perimetral que se deben monitorear con la herramienta LEM, de forma que permite tener reportes más completos y certeros al momento de realizar un análisis de eventos. En la Figura 7 se menciona los dispositivos de seguridad perimetral.

Figura 7. Dispositivos de protección del perímetro



Fuente autor

Entre estos dispositivos se encuentra el Firewall el cual cuenta con una herramienta de almacenamiento y monitoreo de log bastante robusta, dado a la cantidad de eventos que genera y este cuenta con un módulo de análisis de logs en su ambiente web, por ende no se realizará interconexión e instalación de agente de la herramienta LEM.

Para el caso de los dispositivos IPS (*Intrusion Prevention System*) que no se han instalado y por consiguiente su configuración está pendiente de realizarse por parte del proveedor de servicios, se excluye de la instalación de agente LEM y monitoreo desde la herramienta.

5.3.2 Análisis de vulnerabilidades de los activos. Mediante una correcta implementación de dispositivos de seguridad perimetral se obtiene la información básica para el funcionamiento de las herramientas de correlación de eventos o para las soluciones SIEM. La configuración adecuada de estos dispositivos permite ajustar el presupuesto de inversión, sin necesidad de sobre dimensionar las necesidades en dispositivos de seguridad.

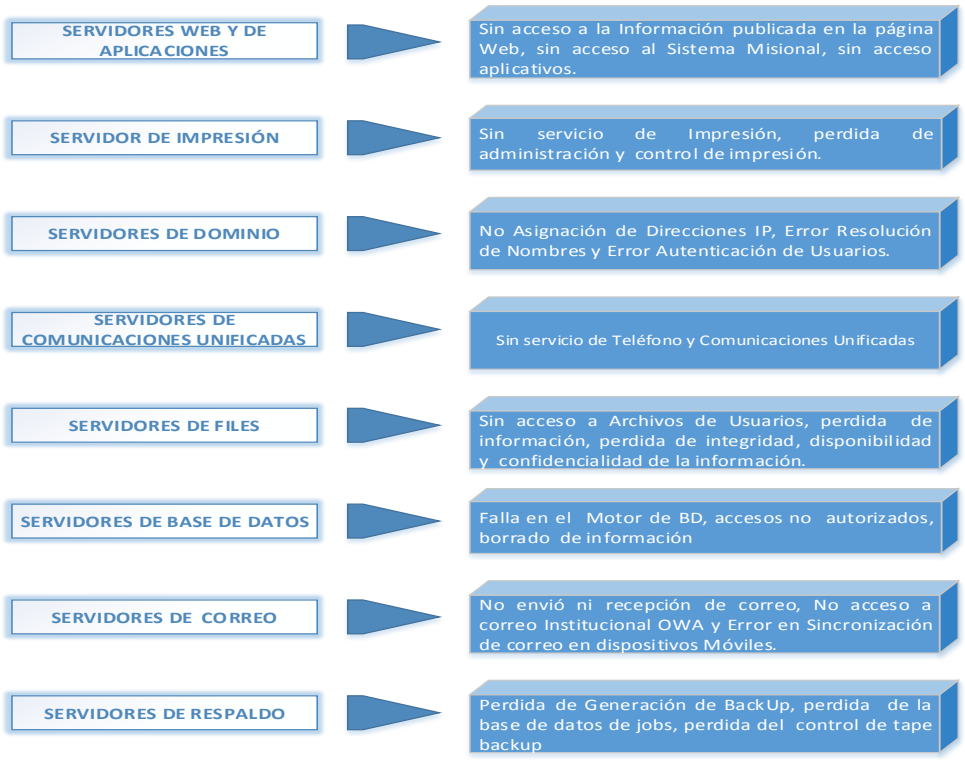
Ahora bien, otro aspecto importante en esta etapa es analizar de manera individual los riesgos para cada uno de los dispositivos puesto que tienen roles diferentes y a su vez facilita la creación de consultas y reportes de forma específica.

Para los dispositivos de seguridad se debe realizar actualizaciones constantes de bases de datos, parametrizarlos con base en las necesidades de la ANSPE y en lo posible tener en alta disponibilidad los dispositivos.

En conclusión, no contar con un análisis de vulnerabilidades implica no conocer los riesgos a los que se encuentra expuesta la ANSPE y un total desconocimiento de la seguridad que se debe implementar o contra qué se debe proteger.

El análisis básico de riesgos de la entidad, se evidencia en la Figura 8 con una descripción gráfica para los servidores en los que se encuentran los servicios principales como correo, acceso a información, aplicaciones para los usuarios, controladores de dominio, etc.

Figura 8. Análisis de riesgos para servidores

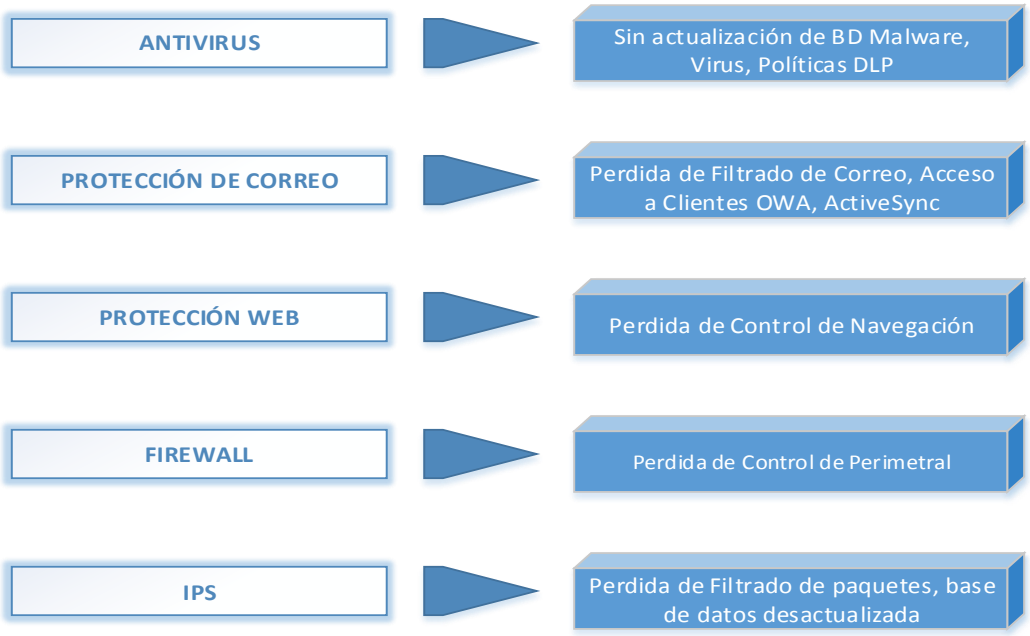


Fuente autor

De igual forma se presenta una imagen con las vulnerabilidades para los dispositivos de seguridad perimetral, los cuales son una fuente de información principal para la correlación de log.

La configuración de reglas y reportes desde la herramienta de LEM permite no solo monitorear si no que prevenir fallas en la seguridad de la información. De igual forma es necesario realizar el análisis de cada una de estas herramientas con su propio colector de información dado que para el caso de los dispositivos McAffe se cuenta con un módulo de reportes en cada una de las herramientas así como el firewall del fabricante Sonic Wall. La Figura 9 muestra los riegos identificados para los dispositivos de seguridad.

Figura 9. Riesgos para dispositivos de seguridad



Fuente autor

5.3.3 Plan de remediación. Con base en la implementación del SGSI se debe definir un plan de mitigación para los riesgos y vulnerabilidades encontrados, ya que no se efectuará una tarea completa sino se realiza un tratamiento adecuado a los riesgos, teniendo en cuenta que estos se conviertan en fallas. El plan de remediación se debe ajustar a todas las vulnerabilidades encontradas, ya sea para mitigar los daños o para una pronta solución y puesta en marcha de los servicios, lo cual ayuda a configurar los equipos de acuerdo a las situaciones reales que se pueden presentar en la agencia.

No obstante, se debe generar una base de conocimiento para el tratamiento de los riesgos con el fin de crear soluciones más eficientes en caso de presentarse nuevamente las fallas o con el fin de realizar análisis futuros.

De igual forma al diseñar planes de remediación se reduce el tiempo de respuesta de los incidentes, lo que se traduce en menores pérdidas para la entidad y garantiza la continuidad del negocio.

5.3.4 Gestión de eventos. En esta etapa se define los responsables de prevenir, actuar y solucionar los eventos que presenten los dispositivos. También se determinan las actividades indicando el tratamiento o escalamiento a realizar para cada uno de los posibles eventos que se presenten.

Para realizar una correcta gestión de eventos la entidad debe contar previamente con la documentación de los activos de información, con los dispositivos de seguridad perimetral que realicen la detección de comportamientos anómalos y de operación normal, con personal idóneo para la gestión de seguridad de la información y con una herramienta de correlación de eventos que permita identificar de forma más rápida el origen de la falla en seguridad o las posibilidades de ocurrencia de un evento.

En el caso de ser posible se deben realizar pruebas periódicas de eventos conocidos para validar las respuesta a los incidentes que se puedan presentar, de forma tal que se analice las soluciones planteadas o los procedimientos a implementar.

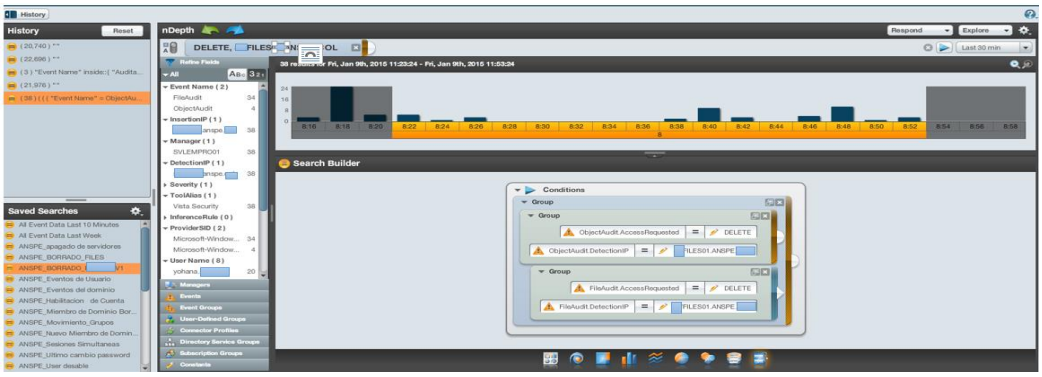
5.4 FASE 4 CORRELACIÓN DE EVENTOS E INFORMES

5.4.1 Correlación de eventos. Una vez se ha realizado la selección de los dispositivos a correlacionar o activos y se ejecuta una adecuada configuración y parametrización de la herramienta SIEM es posible realizar consultas de la información enviada. Correlacionar los eventos, permite analizar de manera eficiente la posible falla presentada, evidenciando el comportamiento en conjunto de los dispositivos y por ende suministrar un informe de ello, se debe tener en cuenta la estandarización y configuración de reglas establecidas en la herramienta. En la Figura 11 se observa la herramienta LEM implementada en la ANSPE, en la cual se realiza un filtrado y correlación de log del servidor de archivos y el controlador de dominio, lo que permite identificar si un archivo ha sido modificado, la fecha y el usuario que lo realizó.

En la Figura 10 se observa la herramienta LEM implementada en la ANSPE, en la cual se realiza un filtrado y correlación de log del servidor de archivos y el

controlador de dominio, lo que permite identificar si un archivo ha sido modificado, la fecha y el usuario que lo realizó.

Figura 10. Configuración herramienta LEM



Fuente software LEM

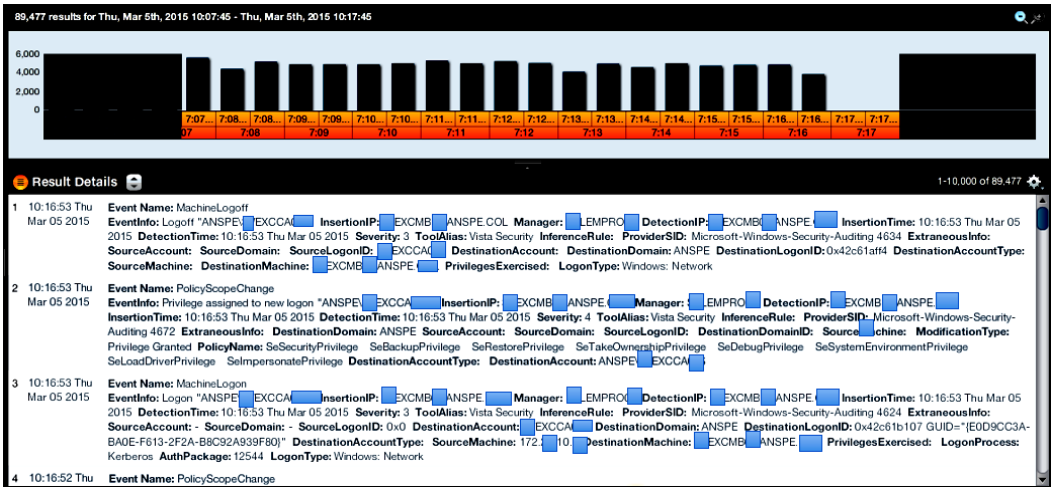
La herramienta cuenta con un dash board de la información actualizada de todos los eventos generados, la cual permite generar de forma gráfica consultas a los logs mediante los parámetros identificados, como se puede evidenciar en la Figura 11.

Figura 11. Parámetros de consulta.

Fuente Software LEM

De igual forma muestra un resumen de todos los eventos generados en un parámetro de tiempo definido por el administrador, lo que permite analizar de forma sencilla los eventos en un tiempo determinado como se muestra en la Figura 12.

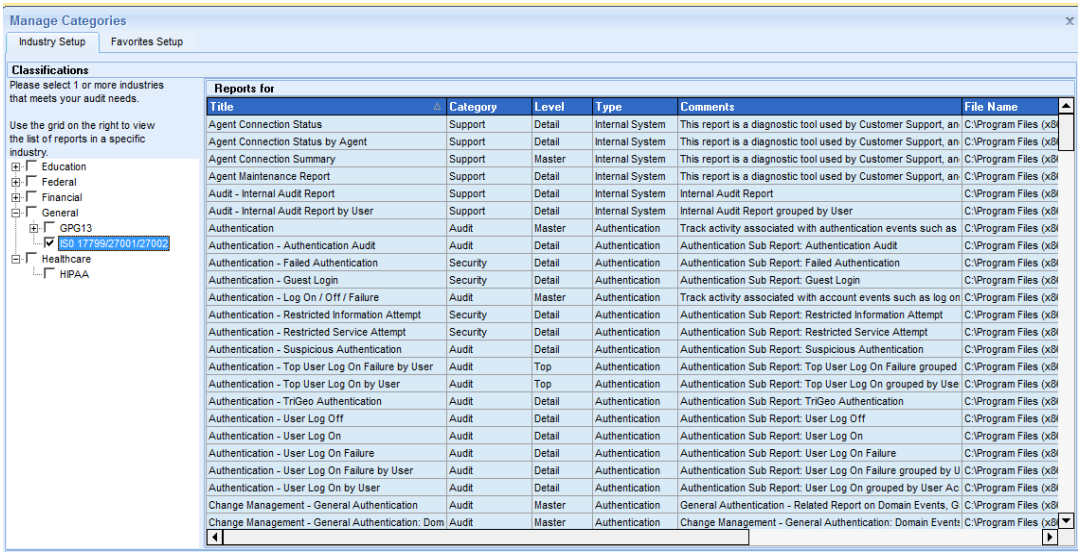
Figura 12. Resumen de eventos.



Fuente Software LEM

5.4.2 Generación de informes. La implementación de la herramienta LEM permite generar reportes de forma rápida en la aplicación WEB, igualmente cuenta con un opción de reportes específicos que se pueden configurar para dar cumplimiento a reportes gerenciales. A su vez contiene un repositorio de bases de informes precargados que se acoplan a normas estandarizadas como la ISO-27001 o ISO-27002 como se puede ver en la Figura 13.

Figura 13. Reporter LEM SolarWinds.



Fuente Software LEM

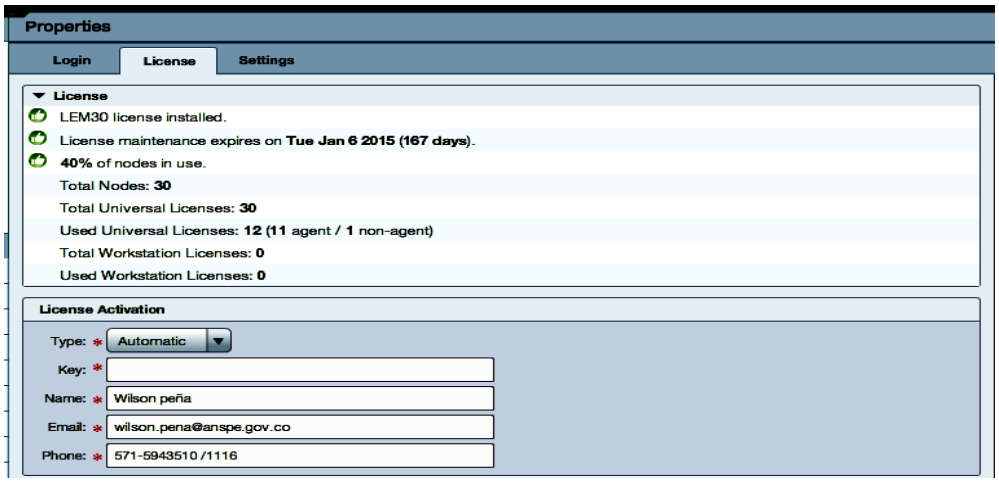
Estos informes que se presentan de forma sencilla son entregados gracias a la configuración de reglas de filtrado de los log almacenados. …en el ANEXO C…se muestra cómo es el proceso para la generación dichas reglas o consultas que entregarán los informes reconfigurados o específicos.

Un valor agregado de los informes basados en la norma, es que facilita el proceso de implementación de SGSI.

5.5 VALIDACIÓN Y ACTUALIZACIÓN DE LA HERRAMIENTA SIEM

A medida que se realiza el proceso de la implementación de SGSI se debe realizar una actualización de la herramienta SIEM ajustánda a los nuevos lineamientos del SGSI. Para el caso práctico del año en curso se debe realizar un ajuste a las normas ISO27000 – 2013 mediante actualizaciones por parte del fabricante. A continuación en la Figura 14, se observa que a través de la herramienta se puede conocer el estado de la licencia.

Figura 14. Licenciamiento LEM.



Fuente Software LEM

La ANSPE cuenta con una licencia de operación y actualización por 1 año, la cual se renueva a través de una compra realizada directamente con los proveedores o desde la página del fabricante (https://customerportal.solarwinds.com/Licenses).

6. CONCLUSIONES

−Luego de realizar los procedimientos indicados en este documento, se obtiene como resultado la implementación de una herramienta de manera eficaz, ya que permite administrar de forma efectiva los log generados por los dispositivos monitoreados.

−La herramienta optimiza el tiempo del grupo de seguridad al disminuir las horas dedicadas a tareas operativas.

−Uno de los beneficios más relevantes es aumentar la seguridad frente a ataques informáticos, evitando fallas en los dispositivos, ya que permite Identificar con prelación comportamientos o eventos sospechosos en ataques de fuerza bruta o malware.

−Se observa que para la implementación de la herramienta SIEM no es necesario tener implementado un SGSI operativo y funcional, sin embargo es necesario tener identificados los activos más relevantes de la entidad junto con sus vulnerabilidades.

−Disminuye el tiempo de identificación, análisis y gestión de los ataques recibidos, gracias a la correlación de logs que se realiza a los equipos en los que se encuentra instalado el agente.

−La implementación de la herramienta mejora la administración de los dispositivos de red y servidores.

−El éxito de la implementación de la herramienta es directamente proporcional la minucia con la que el administrador haya seleccionado los dispositivos que se desean monitorear, así como la definición de las reglas de filtrado y los reportes.

−El apoyo de una norma como la ISO2700 facilita el proceso de implementación de la herramienta.

BIBLIOGRAFÍA

ALIENVAULT. The World´s Most Widely Used Open Source SIEM [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: https://www. alienvault.com/ open-threat-exchange/projects

ARIAS, Luis. COGOLLO, Jhony. Procedimiento para la implementación de una Herramienta SIEM en empresas que cuenten con un sistema de gestión de seguridad de la información. Bogotá. Trabajo de grado. Universidad Piloto de Colombia. Especialización en Seguridad informática. 2013. p. 43.

BABBIN, Jacob et al, Security log managment. Singress. Walthan, MA, USA, 2013. p 4.

CHUVAKIN, Anton et al. Logging and log Management. Syngress. Walthan. MA. USA. 2013. p. 119

CYBEROAM. Intelligent Logging & Reporting. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.cyberoam-iview.org

EMC2. RSA Security Analitics. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://colombia.emc.com/search.htm?fromGlobalSelector#_search/ query:q=SIEM;p:cPage=1

FORD, Verilee. Tecnologías de interconectividad en redes. México: Prentice-Hall.. 1998. p. 645

HP. SIEM. ARCSight ESM. Solución de software. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www8.hp.com/us/en/software-solutions/arcsight-esm-enterprise-security- management/index.html

IBM. IBM QRadar Security Intelligence Platform. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www-03.ibm.com/software/ products/ es/qradar

ISO 27000.es. ¿Qué es un SGSI?. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.iso27000.es/sgsi.html

ITIL como apoyo a la seguridad de la información. [En línea]. [Noviembre 2014] disponible en: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_ JornadaSeguridad/04-ITILSoporte SGSIBasadoISO27001.pdf

KRUEGEL, Chris et al, intrusion detection and correlation: Challengeds and solutions, Santa Barbara, California, USA. Springer, 2005. p.2.
MCAFEE. Email Gateway. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.mcafee.com/us/products/email-gateway.aspx

MCAFEE. Web Gateway. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.mcafee.com/us/products/web-gateway.aspx

MCAFEE. Nitro Security. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.mcafee.com/us/about/mcafee-nitrosecurity.aspx

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Dirección de gobierno en línea. Decreto 1151 de 2008. Articulo 2. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://programa.gobiernoenlinea.gov.co/busquedas.shtml?apc=jxx;x;x;x1-&x=4480

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Dirección de gobierno en línea. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: :http:// programa.gobiernoenlinea. gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/ manual3.1.

REAL ACADEMIA ESPAÑOLA. Definición de antivirus. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://lema.rae.es/drae/?val=antivirus
.
_____. Disponibilidad. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://lema.rae.es/drae/?val=disponibilidad

_____. Integridad. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://lema.rae.es/drae/?val=integridad

_____. ¿Qué es antivirus? [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://lema.rae.es/desen/?key=antivirus

ROEBUCK, Kevi. Data Loss Prevention DLP: High-impact Strategies – What You Need to Know. Emero Pty Limited. 2011. 80 p,

RUSSEL, Charlie; CRAWFORD, Sharon; GEREND, Jason. Guía completa de Microsoft Windows Server 2003 Running+.España: Mc Graw Hill, 2003. p. 171-172.

SIKORSKI, Michael. Practical Malware Analysis. No strach press. San Francisco, CA. USA. 2012. p.28

SIMPLIFIED IT COMPLIANCE. ISO 27002-based Compliance Frameworks RSA Solutions. [En linea]. [Octubre 2 de 2014]. Disponible en: http://colombia.emc.

com/collateral/microsites/ forum 2008/forum2008-security-simplified-it-compliance. pdf

SOLARWINDS. SIEM, Seguridad de la información. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.solarwinds.com/siem-security-information-event-management-software.aspx

SOLARWINDS. LOG & EVENT MANAGER, Generalidades de la empresa. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.solarwinds.com/log-event-manager.aspx

_____. Eventos. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.solarwinds.com/log-event-manager.aspx

SOLARWINDS. SOLARWINDS LOG & EVENT MANAGER, Datasheets. [en línea]. [consultado el 25 de julio de 2014]. Disponible en: http://web.swcdn.net/creative/pdf/ datasheets/ SW_LEM_ Datasheet.pdf

SWIFT David, A practical Application of SIM/SEM/SIEM Automating Threat Identification. SANS USA: Institute Infosec Reading Room, 2007 p.19.

TORRES, Juan Carlos; RONDÓN, Richard "Control, Administración e Integridad de Logs." [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://www.criptored. upm.es/guiateoria/gt_m248h.htm

VAN BON, Jan. Fundamentos de la gestión de servicios de TI basada en ITIL. 1ra Edición. Amersfoot.: Van Haren Publishing Zaltbommel, 2008.

VICENTE, Carlos. "Gestión de Traps SNMP" [en línea], [Consultado el 23 de octubre de 2014]. Disponible en: https://www.nsrc.org/workshops/2008/walc/ presentaciones/gestion_traps.pdf

WINDOWS. MICROSOFT. ¿Que es un firewall?. [en línea], [Consultado el 23 de Noviembre de 2014]. Disponible en: http://windows.microsoft.com/es-co/windows/what-is-firewall#1TC=windows-

ANEXO A

IMPLEMENTACIÓN HERRAMIENTA LEM

Al realizar el análisis de las herramientas de recolección de logs la Agencia Nacional para la Superación de la Pobreza Extrema (ANSPE) adquiere el dispositivo LEM del fabricante SolarWinds que corresponde a una herramienta de recolección de logs SIEM para este fabricante.

La implementación de una herramienta SIEM se realiza con el objetivo de correlacionar los eventos, aumentar la protección de los activos de información y dar una mayor seguridad a la información.

El cuadro 5 describe las características técnicas requeridas para la implementación de esta herramienta[36]:

Cuadro 5. Requerimientos mínimos de instalación

HARDWARE	REQUERIMIENTOS MINIMOS
CPU	Procesador Dual, 3.0 GHz
MEMORIA	8 GB RAM
DISCO DURO	250 GB
SOFTWARE	**REQUERIMIENTOS MINIMOS**
SISTEMA OPERATIVO	Vmware ESX / ESXi 4.0 ó superior Hyper-V Server 2008, 2008 R2, 2012, 2012 R2
BASE DE DATOS	Integrada con la máquina virtual
Fuente Pagina web Solarwinds	

El acceso a la herramienta es mediante un entorno WEB que permite un mayor acceso y facilidad de configuración.

Dado que la ASPE cuenta con un SGSI en proceso de implementación y desarrollo, en el cual se está adelantando los procesos de levantamiento de información para la selección de activos y fortalecimiento de las medidas de seguridad, se realiza la

[36] SOLARWINDS. SOLARWINDS LOG & EVENT MANAGER, Datasheets. [en línea]. [consultado el 25 de julio de 2014]. Disponible en: http://web.swcdn.net/creative/pdf/ datasheets/ SW_LEM_Datasheet.pdf

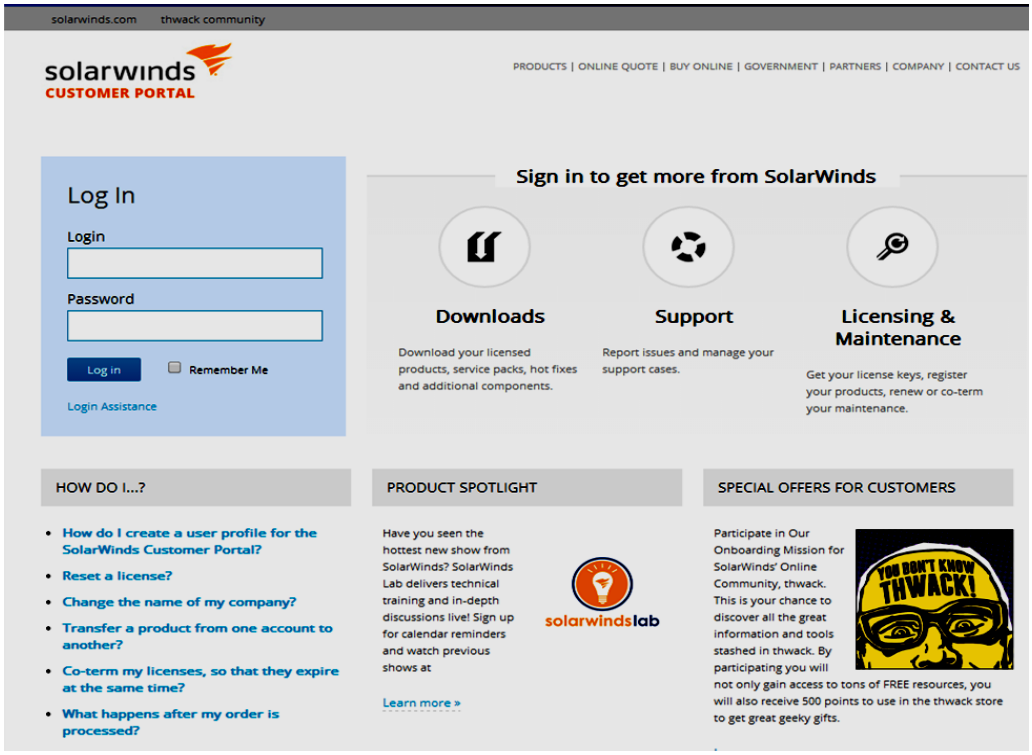
clasificación y el análisis de los dispositivos que son monitoreados por la herramienta SIEM, así como sus vulnerabilidades.

El proceso de instalación de la herramienta LEM se describe a continuación, en primer lugar se debe Instalar el software en el servidor con las características técnicas mencionadas ver…Figura 15… el segundo paso es proceder con:

A.1 ACTIVACIÓN DE LICENCIA

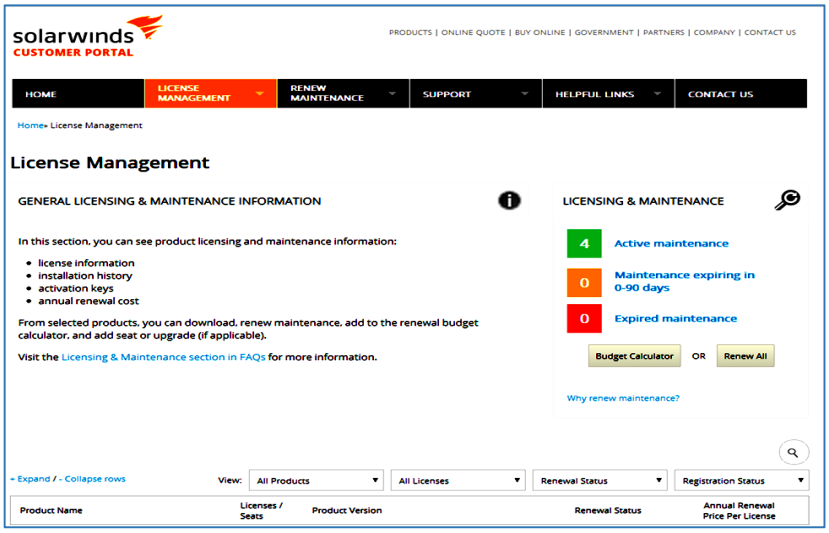
Para activar licencia de la herramienta LEM de debe ingresar a la página Web: https://customerportal.solarwinds.com/Licensesymediante la creación de un usuario se realiza la descarga del software para la instalación de agentes, software de administración o actualizaciones, como se observa en las ilustraciones 15 y 16. La herramienta cuenta con un software para realizar periodos de prueba de la solución SIEM, permite a futuros usuarios realizar una implementación para validar la inversión de la misma.

Figura 15. Página del fabricante SolarWinds



Fuente Pagina web Solarwinds

Figura 16. Página de activación software LEM.

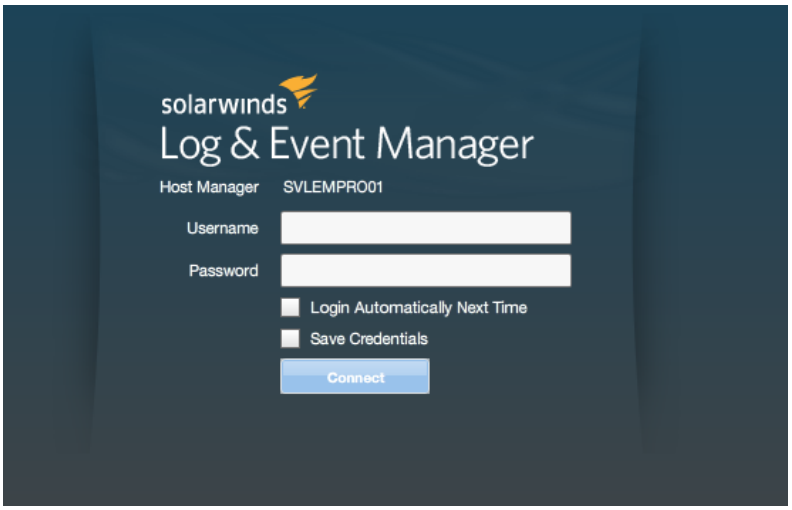


Fuente página web Solarwinds

Al descargar el software de la herramienta, se debe ejecutar sobre el servidor con las características técnicas descritas anteriormente.

La Figura 17 evidencia la ventana de autenticación, la cual permite el inicio de sesión web, una vez se instale la herramienta.

Figura 17. Acceso WEB a LEM



Fuente Herramienta LEM

Mediante el uso de la consola se crean los parámetros de acceso para el administrador de la herramienta, la cual debe ser administrada desde el ambiente web, donde se observa sus componentes entre los que se encuentra los enlaces a varios módulos, como se puede observar en la Figura 18.

Figura 18. Módulos herramienta LEM

Fuente Herramienta LEM

A.2 COMPONENTES HERRAMIENTA LEM

Las características principales de los diferentes módulos se describen A continuación.

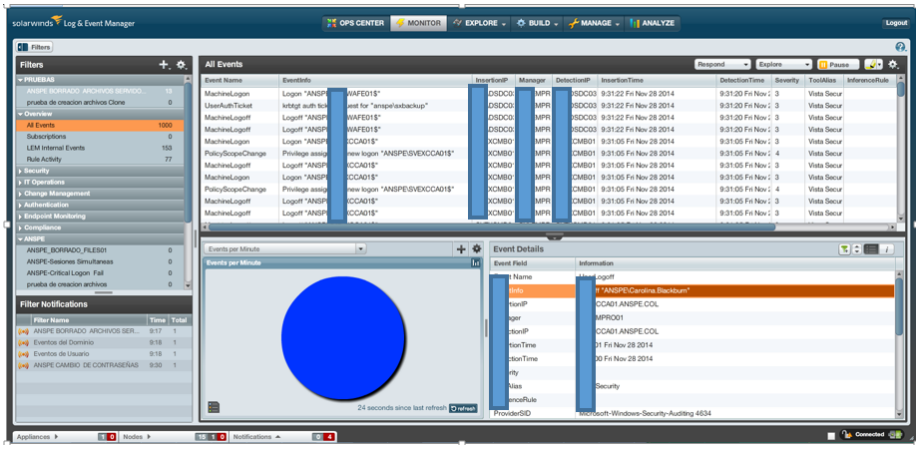
A.2.1 OPS Center. La herramienta cuenta con varios tipos de reportes entre los cuales se encuentran previamente parametrizados algunos, tales como los que se puede observar en la Figura 19: el top 10 de eventos, casos más recurrentes, estados de los agentes, entre otros.

Figura 19. OPS center

Fuente Herramienta LEM

A.2.2 Monitor. En esta dashboard se encuentra las consultas precargadas de la herramienta, así como las generadas por el administrador, de igual forma se muestra el monitoreo constante a los dispositivos. En la Figura 20 se observa la ventana de monitoreo de la herramienta.

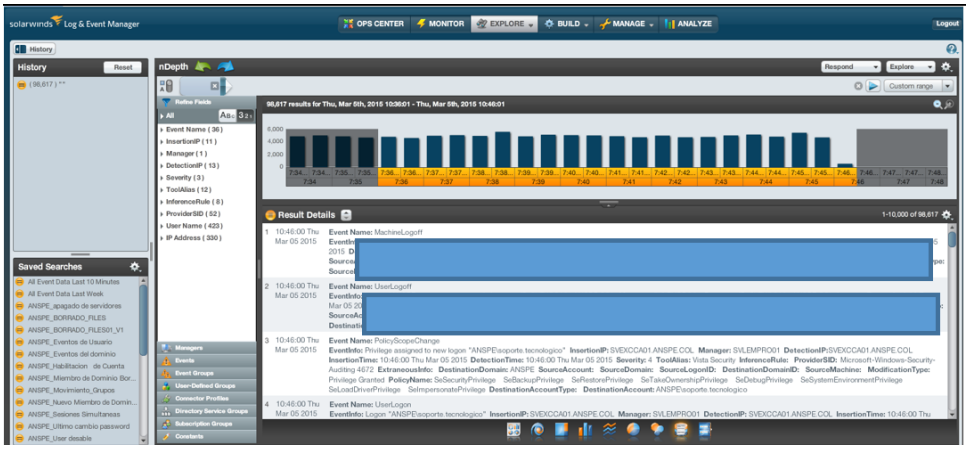
Figura 20. Monitor



Fuente Herramienta LEM

A.2.3 Explore. Permite realizar consultas en tiempo real sobre la información almacenada, las cuales se puede estandarizar su periodicidad para que se generen de manera frecuente o esporádica. En la Figura 21 se visualiza la interface de este módulo.

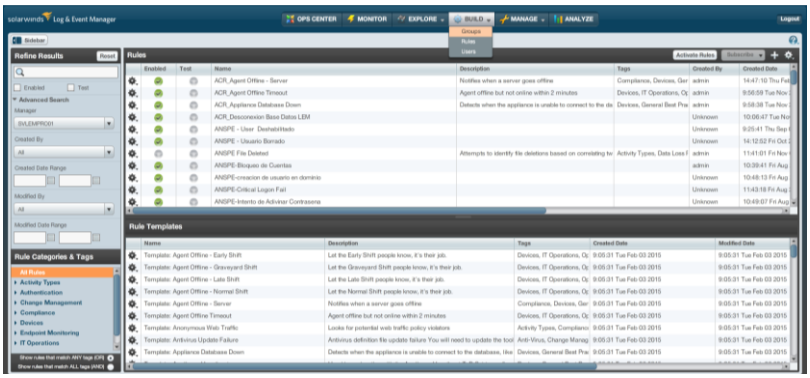
Figura 21. Explore



Fuente Herramienta LEM

A.2.4 Build. Este módulo permite la creación de usuarios y reglas de filtrado, para parametrizar la herramienta y por ende las consultas que estos pueden generar. En la Figura 22 se observa la ventana correspondiente a este módulo,

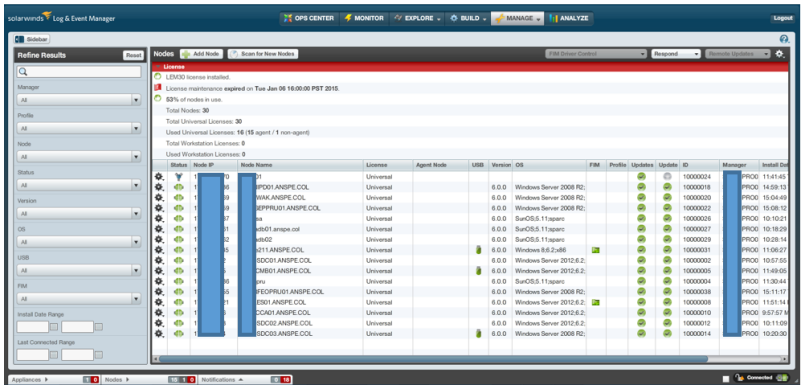
Figura 22. Build



Fuente Herramienta LEM

A.2.5 Manage. Este módulo permite la administración de nodos y de las consolas instaladas. Como se observa en la Figura 23. De igual forma entrega la información de los nodos y la licencia de la herramienta.

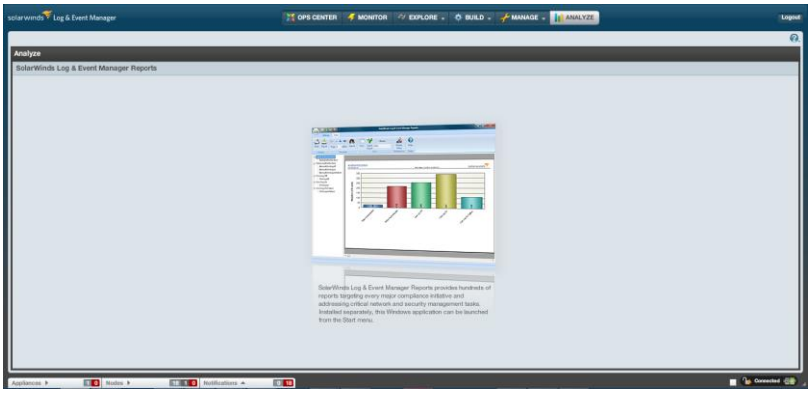
Figura 23. Manager



Fuente Herramienta LEM

A.2.6 Analyze. Este módulo cuenta con la integración de un reporteador para la generación de informes configurados o para realizar informes específicos. En la Figura 24 se puede observar un gráfico de un reporte específico.

Figura 24. Analyze

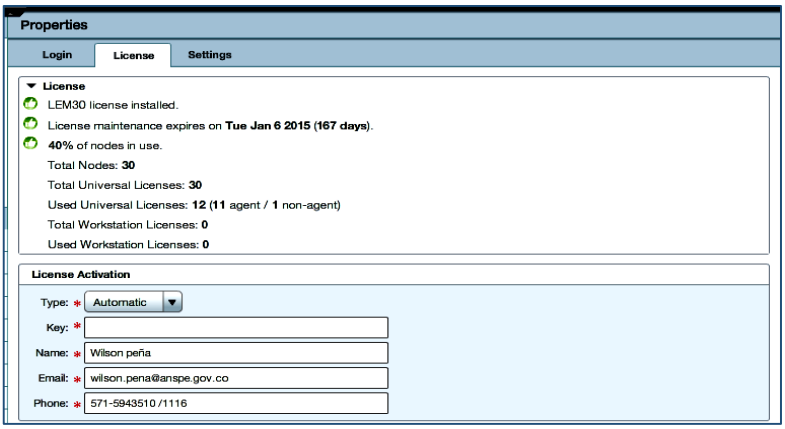


Fuente Herramienta LEM

A.3 CARACTERISTICAS HERRAMIENTA LEM

Una vez instalada la herramienta se puede validar sus características, como es el número de licencias de agente, total de nodos, consolas, entre otras, a través de la opción propiedades, como se observa en la Figura 25:

Figura 25. Validación licenciamiento LEM.

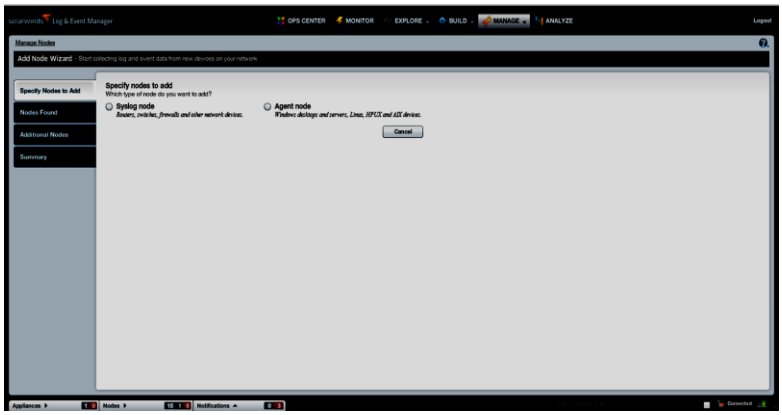


Fuente Herramienta LEM

Una vez finalizada la instalación del software se da inicio al proceso de configuración, donde parte de este procedimiento es desplegar agentes en los dispositivos para capturar y analizar la información del Log que estos generan.

La Herramienta LEM de SolarWinds basa su conexión con los equipos de red en la instalación de un agente, siempre y cuando el sistema operativo lo permita, de lo contrario se debe realizar una conexión por protocolos o conectores de SNMP y SYSLOG. En la Figura 26 se observa la opción de instalación del agente.

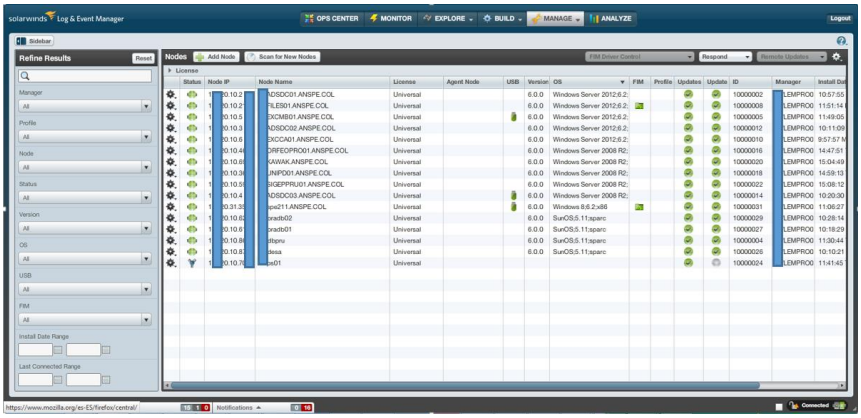
Figura 26. Opciones de instalación agente LEM.



Fuente Herramienta LEM

A medida que se instalan los agentes o se configuren los conectores de los dispositivos a monitorear, se puede observar en el dashboard de nodos la recolección de logs como se muestra en la Figura 27.

Figura 27. Agentes instalados en ANSPE.



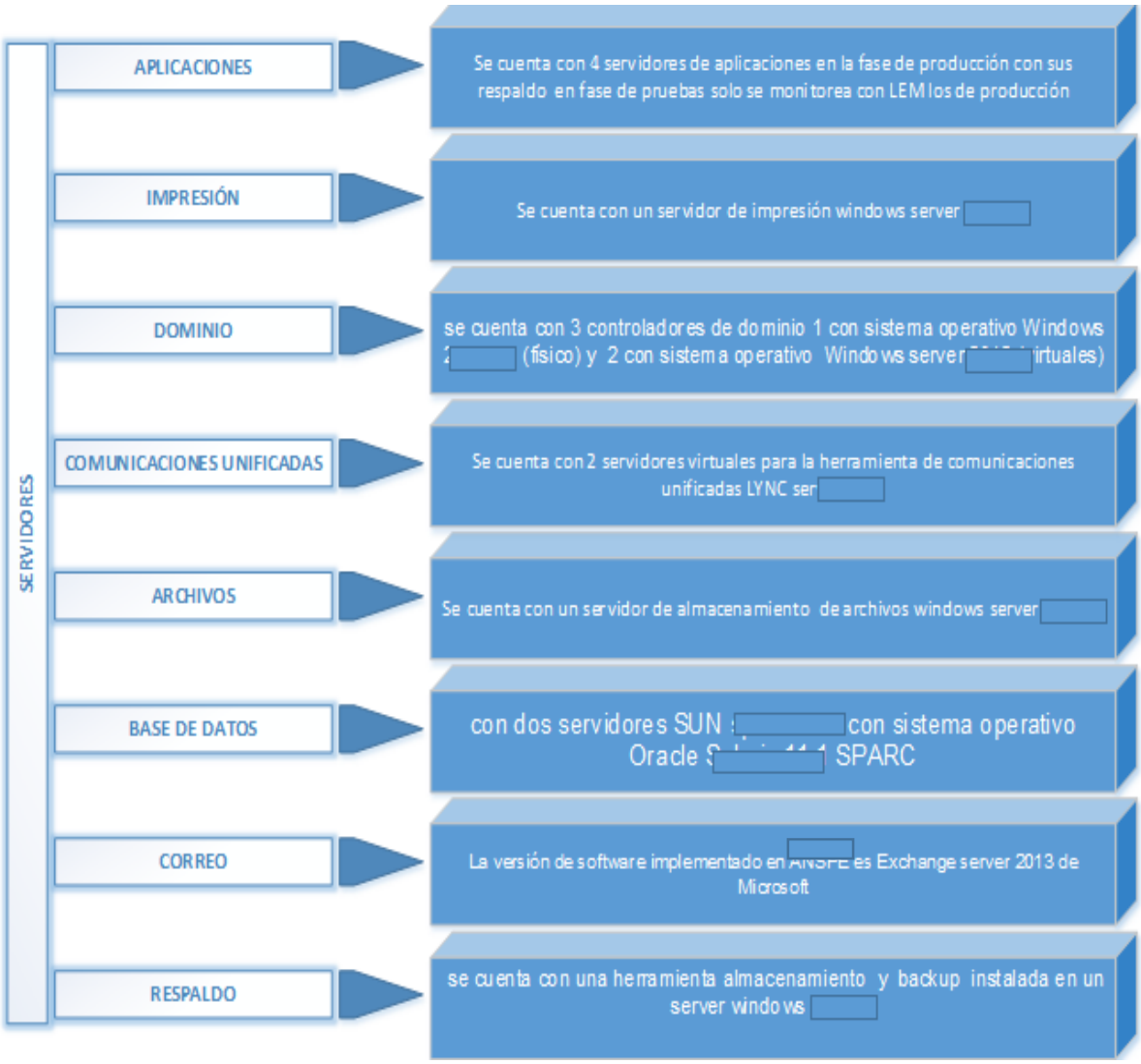
Fuente Herramienta LEM

El licenciamiento de ANSPE permite la instalación y monitoreo para 30 dispositivos.

En la selección de dispositivos de origen realizada en la ANSPE y de acuerdo al avance del SGSI, se obtiene como resultado los siguientes:

A.3.1 Servidores. Se realiza la valoración de los servidores y aplicaciones críticas para la ANSPE los cuales se observan en la Figura 28.

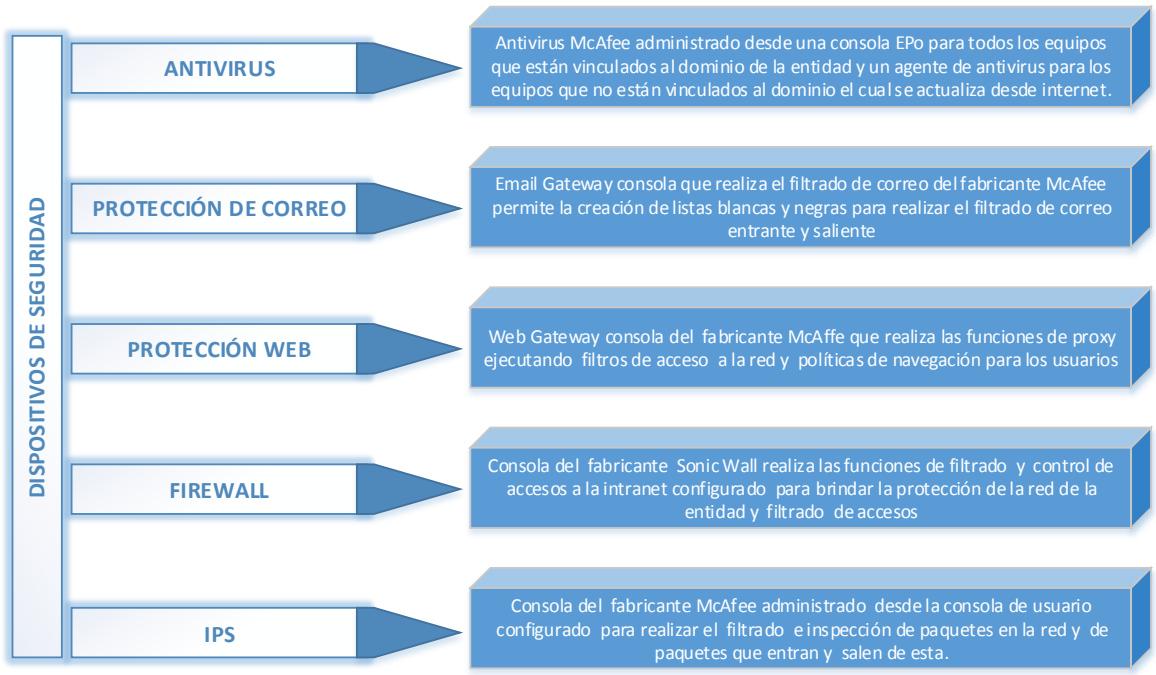
Figura 28. Servidores ANSPE.



Fuente autor

A.3.2 Dispositivos de seguridad. Son elementos físicos o software configurados en la red de la entidad que permiten contrarrestar y mitigar el acceso no autorizado a los activos de información más relevantes de la entidad. Los elementos con los que cuenta ANSPE a la fecha se evidencian en la Figura 29, que se muestra a continuación:

Figura 29. Dispositivos de seguridad ANSPE.



Fuente autor

ANEXO B

INSTALACIÓN AGENTES LEM

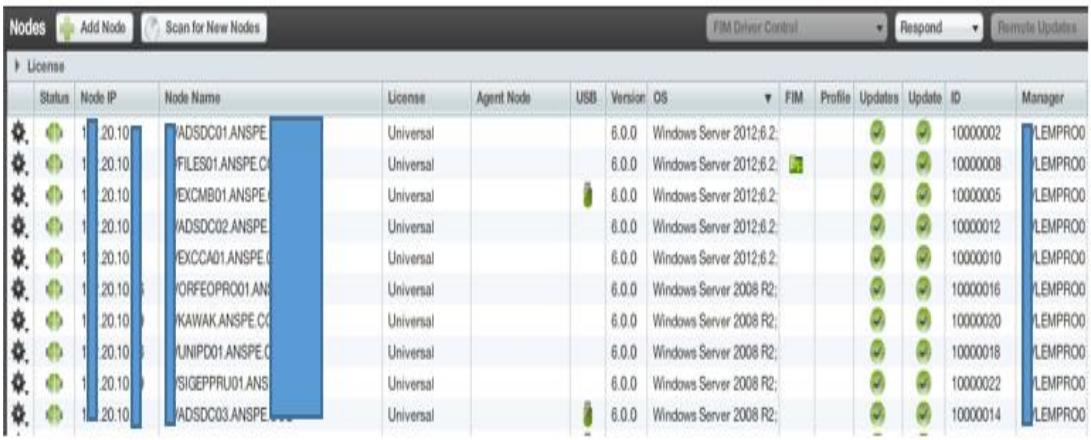
En este anexo se podrá evidenciar la instalación de agentes para los diferentes sistemas operativos.

B.1 SISTEMA OPERATIVO WINDOWS

Para este sistema operativo se cuenta con un ambiente grafico que permite realizar paso a paso y de forma sencilla la instalación del agente para la herramienta LEM del fabricante SolarWinds, o cual se puede evidenciar en la Figura 30.

El proceso inicia con la descarga del software de la página del fabricante. http://www.solarwinds.com/es/log-event-manager.aspx

Figura 30. Agentes instalados en Windows.

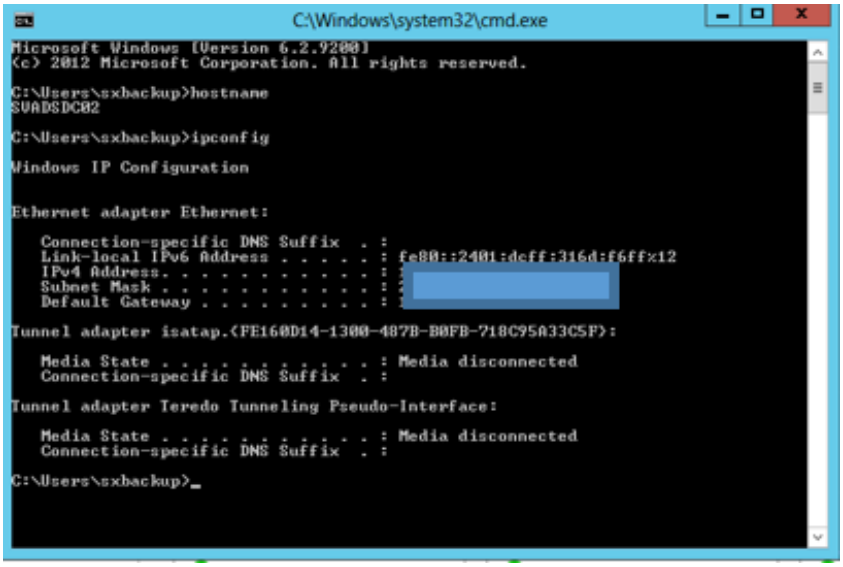


Fuente Herramienta LEM

B.2.1 Procedimiento de instalacion de agentes LEM. A continuación se describe la instalación de un agente LEM en un servidor controlador de dominio de forma sencilla y pasó a paso.

En primera instancia se valida la direccion IP del dispositivo en el que se realizará la instalacion del Agente LEM, como se observa en la Figura 31.

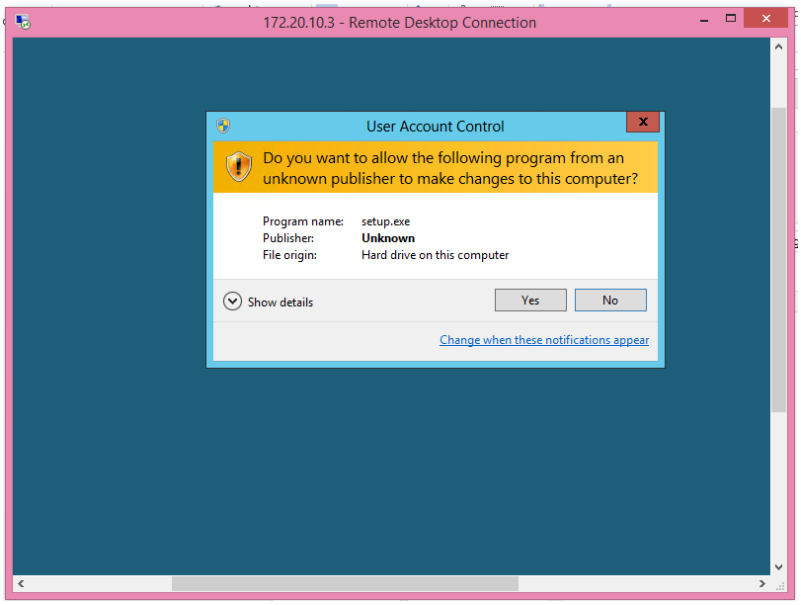
Figura 31. Agentes instalados en Windows.



Fuente Ventana CMD Windows

La Figura 32 evidencia la ventana de ejecución para la instalación de software en el sistema operativo de Windows.

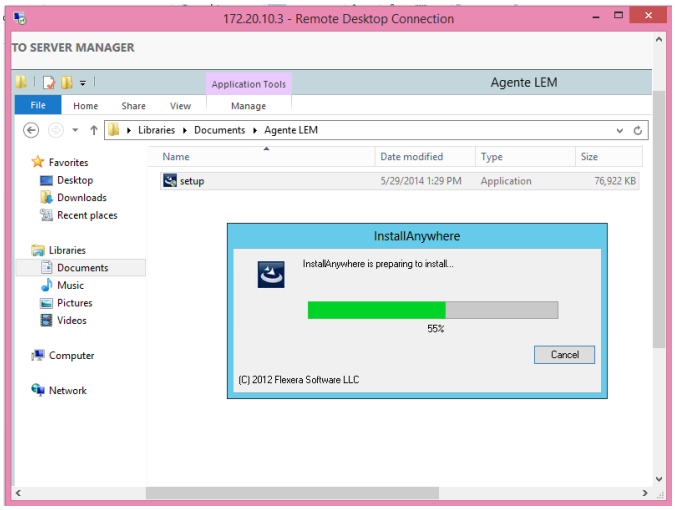
Figura 32. Instalador Software LEM



Fuente Ventana Windows

Se ejecuta archivo.exe descargado de la pagina: http://www.solarwinds.com/es/log-event-manager.aspx, como se muestra en la Figura 33.

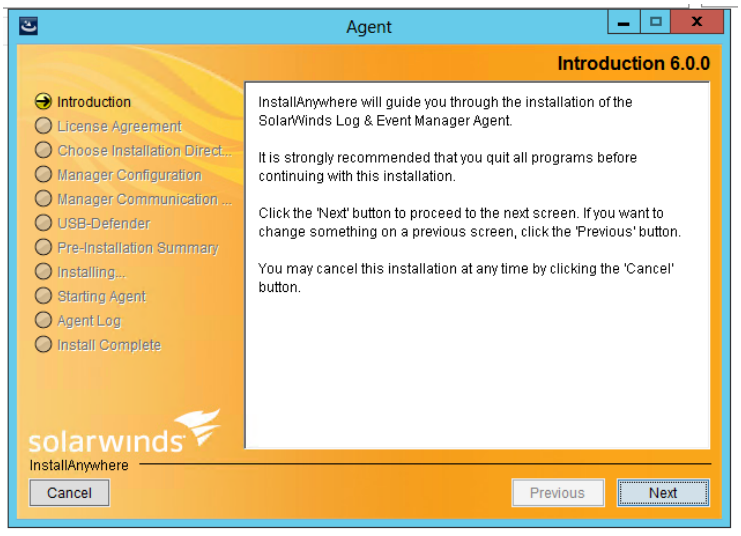
Figura 33. Archivo .exe software LEM



Fuente Ventana Windows

En la introdución se recomienda no tener abiertos más programas y continuar con el proceso por medio de la ventana evidenciada en la Figura 34.

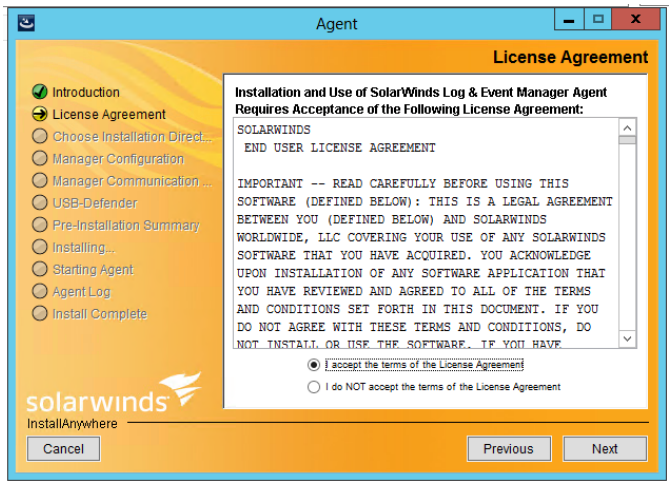
Figura 34. Inicio de instalación LEM



Fuente Ventana instalación agente LEM

En la Figura 35, se evidencia los requerimientos legales para la instalación y manipulación de la herramienta LEM, los cuales deben ser aceptados por el cliente.

Figura 35. Requerimientos legales de LEM.



Fuente Ventana instalación agente LEM

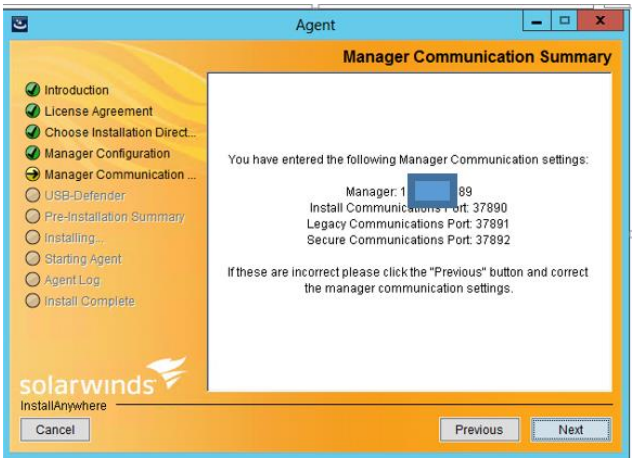
Se debe solicitar al adminstrador la direccion IP de la consola y los puertos por los que se realiza la comunicación del agente de LEM. Esta información se diligencia en la ventana que se muestra en la Figura 36.

Figura 36. Configuración IP de LEM.

Fuente Ventana instalación agente LEM

Luego de confirmar los datos entregados por el adminstrador, muestra un resumen del direccionamiento y puertos configurados. Esto se observa en una ventana como la relacionada en la Figura 37.

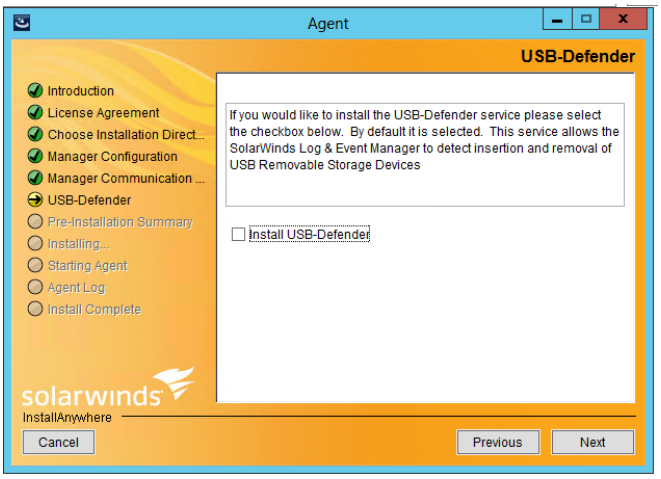
Figura 37. Confirmación de puertos.



Fuente Ventana instalación agente LEM

Para el caso de dispositivos con puertos perféricos USB se puede optar por instalar o no el monitoreo de estos. Lo recomendado por la herramienta es realizarlo para servidores de archivos y base de datos. Este proceso se realiza como se muestra en la Figura 38.

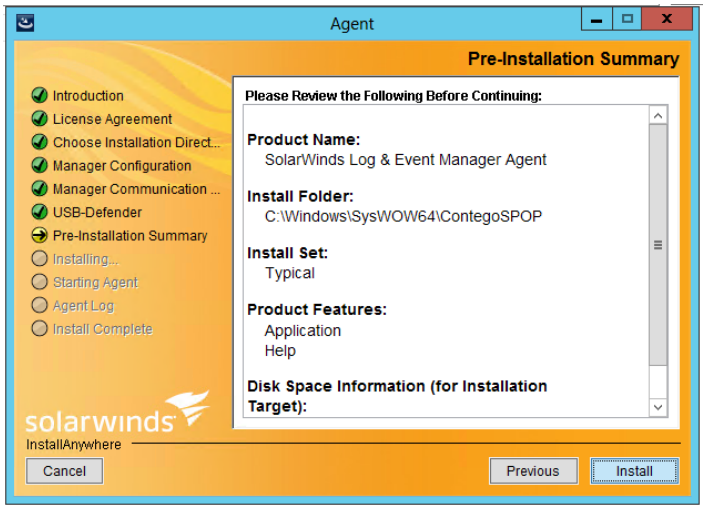
Figura 38. Validación monitoreo puertos USB.



Fuente Ventana instalación agente LEM

En la Figura 39 se evidencia que la herramienta entrega un resumen de las configuraciones realizadas por el administrador en los pasos anteriores, asi como las características del tipo de instalacion del agente de LEM.

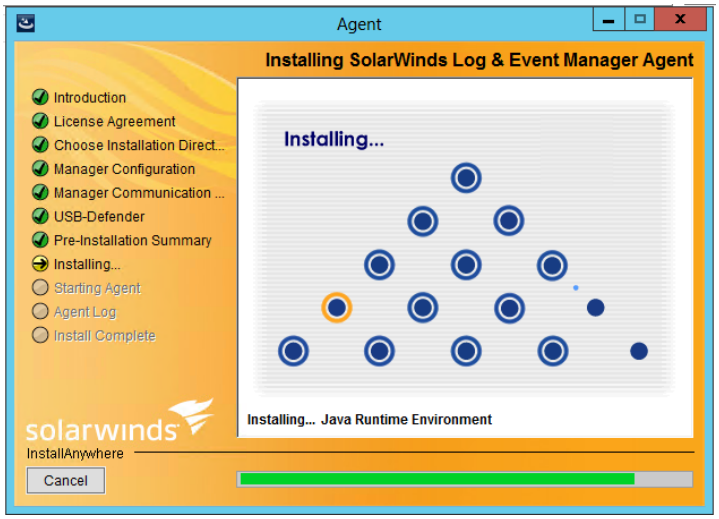
Figura 39. Resumen de configuración LEM.



Fuente Ventana instalación agente LEM

Al iniciar el proceso de instalacion del Agente se validan las caracteristicas del servidor destino y la conexión con la consola. Como se visualiza en la Figura 40.

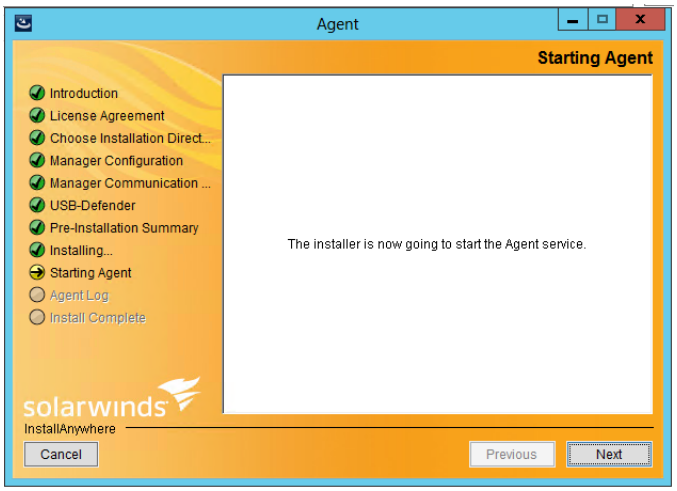
Figura 40. Validación de características.



Fuente Ventana instalación agente LEM

En la Figura 41, se observa el inicio de la ejecución y comunicación con el servidor LEM.

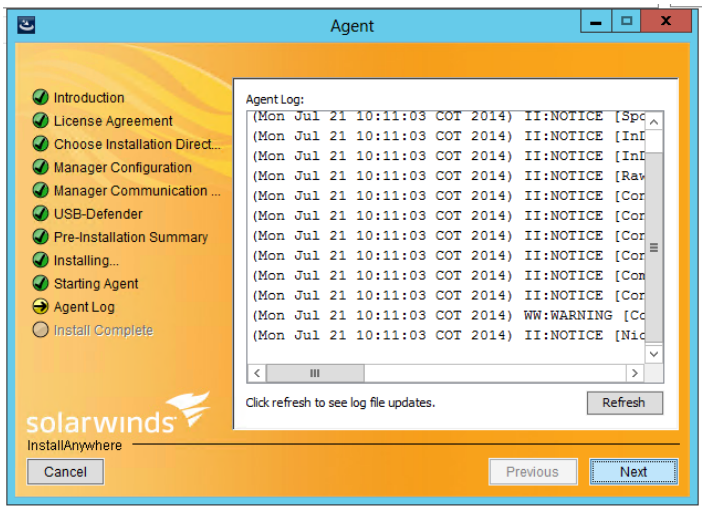
Figura 41. Comunicación y transferencia Agente LEM.



Fuente Ventana instalación agente LEM

La Figura 42 muestra el proceso de configuración y logs creados en el momento de configurar e instalar el agente.

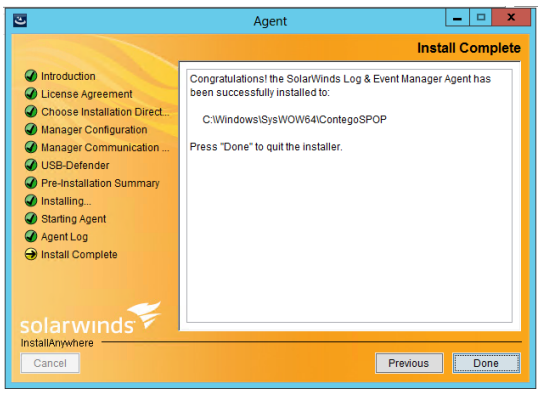
Figura 42. Proceso de configuración LEM.



Fuente Ventana instalación agente LEM

La ventana de finalización de la instalación del Agente, es la evidencia en la Figura 43.

Figura 43. Validación de instalación agente LEM.



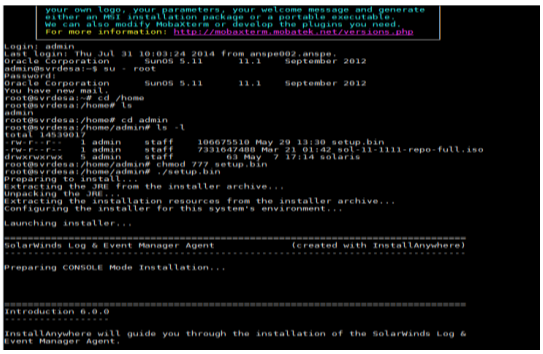
Fuente Ventana instalación agente LEM

B.2 SISTEMA OPERATIVO UNIX/LINUX

Para el caso de un sistema operativo Unix se debe contar con conocimientos previos de los comandos y permiso de administrador en el dispositivo para realizar la instalación.

En la Figura 44 se realiza una descripción gráfica de la instalación de un agente de LEM en un sistema operativo UNIX.

Figura 44. Instalación agente LEM en UNIX



Fuente Servidor Solaris

El resultado del proceso de instalación, una vez se ejecuta, muestra lo siguiente:

root@svrdesa:/home/admin# ./setup.bin
Preparing to install...
Extracting the JRE from the installer archive.
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Launching installer...
==========
SolarWinds Log & Event Manager Agent (created with InstallAnywhere)

Preparing CONSOLE Mode Installation...
==========
Introduction 6.0.0

InstallAnywhere will guide you through the installation of the SolarWinds Log & Event Manager Agent.
It is strongly recommended that you quit all programs before continuing with this installation.
Respond to each prompt to proceed to the next step in the installation. If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.
PRESS <ENTER> TO CONTINUE:
==========
License Agreement

Installation and use of SolarWinds Log & Event Manager Agent requires acceptance of the following License Agreement:
SOLARWINDS
END USER LICENSE AGREEMENT
IMPORTANT -- READ CAREFULLY BEFORE USING THIS SOFTWARE (DEFINED BELOW): THIS IS
A LEGAL AGREEMENT BETWEEN YOU (DEFINED BELOW) AND SOLARWINDS WORLDWIDE, LLC
COVERING YOUR USE OF ANY SOLARWINDS SOFTWARE THAT YOU HAVE ACQUIRED. YOU
ACKNOWLEDGE UPON INSTALLATION OF ANY SOFTWARE APPLICATION THAT YOU HAVE
REVIEWED AND AGREED TO ALL OF THE TERMS AND CONDITIONS SET FORTH IN THIS

DOCUMENT. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, DO NOT INSTALL
OR USE THE SOFTWARE. IF YOU HAVE ALREADY INSTALLED THIS SOFTWARE AND DO NOT
AGREE TO THESE TERMS AND CONDITIONS, PLEASE UNINSTALL THE SOFTWARE AND
IMMEDIATELY DISCONTINUE ITS USE. YOU AGREE THAT YOUR USE OF THE SOFTWARE
ACKNOWLEDGES THAT YOU HAVE READ THIS LICENSE, UNDERSTAND IT, AND AGREE TO
COMPLY WITH ITS TERMS AND CONDITIONS.
BY CLICKING ON THE "ACCEPT" BUTTON, OPENING THE PACKAGE, DOWNLOADING THE
PRODUCT, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING
TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS
AGREEMENT, CLICK THE "DO NOT ACCEPT" BUTTON AND THE INSTALLATION PROCESS WILL
NOT CONTINUE. IN ADDITION, (1) IF YOU ARE OTHERWISE ATTEMPTING TO DOWNLOAD THE
PRODUCT AND YOU DO NOT AGREE WITH THE TERMS OF THIS AGREEMENT, DO NOT COMPLETE
THE DOWNLOAD; OR (2) IF YOUR SOFTWARE WAS INCLUDED IN EQUIPMENT WHICH YOU
PURCHASED AND YOU DO NOT AGREE WITH THE TERMS OF THIS AGREEMENT, DO NOT USE THE
SOFTWARE.
PRESS <ENTER> TO CONTINUE:

This End User License Agreement (the "EULA") is hereby entered into and agreed upon by You, either an individual or an entity ("You" or "Company") and SolarWinds Worldwide, LLC and its affiliates, directors, officers, agents, employees, and its suppliers and licensors (collectively "SolarWinds") for the Software (as defined below).
1. DEFINITIONS.
1.1 "Software" means the object code versions of the product, together with the updates, upgrades, modifications or enhancements owned and provided by SolarWinds to You pursuant to this EULA.
1.2 "Computer" means the hardware, if the hardware is a single computer system whether physical or virtual, or shall mean the computer system with which the hardware operates, if the hardware is a computer system component.
2. GENERAL USE.
2.1 Individual Components. This Software is an application made up of

individual software components, each of which was individually written and copyrighted.
PRESS <ENTER> TO CONTINUE:
2.2 Third Party Software and/or Components. ANY THIRD PARTY SOFTWARE, INCLUDING ANY THIRD PARTY'S PLUG-IN, THAT MAY BE PROVIDED WITH THE SOFTWARE IS
INCLUDED FOR USE AT YOUR OPTION. IF YOU CHOOSE TO USE SUCH THIRD PARTY
SOFTWARE, THEN SUCH USE SHALL BE GOVERNED BY SUCH THIRD PARTY'S LICENSE
AGREEMENT. SOLARWINDS IS NOT RESPONSIBLE FOR ANY THIRD PARTY'S SOFTWARE AND
SHALL HAVE NO LIABILITY FOR YOUR USE OF THIRD PARTY SOFTWARE. YOU MAY ACCESS
ANY THIRD PARTY LICENSE INCLUDED WITH THE SOFTWARE YOU HAVE PURCHASED AT
http://www.solarwinds.com/support/3rdPartySoftware/3rdParty.htm.
The third-party software contained in this Software may include or contain software licensed under the following licenses, GNU General Public License (�GPL�) or Lesser GNU General Public License (�Open Source Programs�). These
Open Source Programs are licensed pursuant to an end user license agreement that permits the end user to copy, modify, and redistribute the software, in both source code and binary code forms. These end user license agreements can be located at: http://www.solarwinds.com/support/3rdPartySoftware/3rdParty.htm. Nothing in this EULA limits an end user�s rights under, or grants the end user rights that supersede, the terms of any applicable Open Source Program end user license agreement.
2.3 Collective Work. The Software is a collective work under U.S. Copyright Law. Upon installation of this Software, SolarWinds hereby grants You the following license to use the Software in Your facility subject to the terms
PRESS <ENTER> TO CONTINUE:
contained herein subject to the licenses referenced herein.
3. GRANT OF LICENSE. Upon payment of the fees applicable under this EULA, SolarWinds hereby grants to You a perpetual, non-exclusive, nontransferable license to use the Software and any related documentation ("Documentation"), subject to the following terms:
a) For each registered serial number and Software license key that you purchase, You may: (i) use the Software on any single Computer; and (ii) copy the Software for back-up and archival purposes, provided any copy must contain all of the original Software's proprietary notices within the United States and its territories or any other country to which this program can legally be exported.
b) The Software is "in use" on a Computer when it is loaded into temporary

memory or installed in permanent memory (Hard Drive, CD-ROM or other storage device). You agree to use Your best efforts to prevent and protect the contents of the Software and Documentation from unauthorized use or disclosure. You agree that You will register this Software and its corresponding serial number only with SolarWinds and that You will only install a Software license key obtained directly from SolarWinds.
PRESS <ENTER> TO CONTINUE:

4. LICENSE RESTRICTIONS.
4.1 You may not: (i) permit other individuals to use the Software or Documentation except under the terms listed above; (ii) modify, translate, reverse engineer, decompile, disassemble (except to the extent that this restriction is expressly prohibited by law) or create derivative works based upon the Software or Documentation; (iii) copy the Software or Documentation (except for back-up or archival purposes); (iv) rent, lease, transfer, or otherwise transfer rights to the Software or Documentation; or (v) remove any proprietary notices or labels on the Software or Documentation. Any such forbidden use shall immediately terminate Your license to the Software. The recording, playback and download features of the Software are intended only for use with public domain or properly licensed content and content creation tools.
You may require a third party license to create, copy, download, record or save third-party media or content files for playback by this Software or to serve or distribute such files to be played back by the Software.
4.2 SolarWinds Name. You may not delete, remove, hide, move or alter any icon, image or text that represents the company name of SolarWinds, any derivation thereof, or any icon, image, or text that is likely to be confused with the same. *All representations to the company name* *SolarWinds* *must remain as originally distributed regardless of the presence or absence of a trademark,*

PRESS <ENTER> TO CONTINUE:

copyright, or other intellectual property symbol or notice requirement.

4.3 Export Restrictions. The Software (including encryption software) and Documentation (including any technical data) delivered to You under this EULA are subject to U.S. export control laws and regulations and may also be subject to import and export laws of the jurisdiction in which it was obtained, if outside the U.S. You shall abide by all applicable export control laws, rules and regulations applicable to the Software and Documentation. You agree that You will not export, re-export, or transfer the Software or Documentation, in whole or in part, to any country, person, or entity subject to U.S. export restrictions. You specifically agree not to export, re-export, or transfer the S00000oftware or Documentation (i) to any country to which the U.S. has embargoed or restricted the export of goods or services, or to any national of any such country, wherever located, who intends to transmit or transport

the products back to such country; (ii) to any person or entity who You know or have reason
to know will utilize the Software or portion thereof in the design, development, production or use of nuclear, chemical or biological materials, facilities, or weapons; or (iii) to any person or entity who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government.
4.4 Compliance with Applicable Laws. You agree that You shall only use the
PRESS <ENTER> TO CONTINUE:
Software and Documentation in a manner that complies with all applicable laws in the jurisdictions in which You use the Software and Documentation, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.
4.5 Use by Network Monitoring Services Providers. SolarWinds strictly prohibits the use of the Software to sell or provide network monitoring services to users who are not individually licensed by SolarWinds except as described herein:
(a) If You represent a Web Hosting company (also referred to as managed service providers, internet service providers, or xSPs), You may use the Software to test and report the applications, servers and equipment resources You use to provide hosting services to Your customers; or
(b) If You operate a data center or provide infrastructure services, You may use the Software to test and report applications, servers and equipment whether such Resources are owned by You or Your customers.
If You are an IT consultant, IT solution provider, or facilities management provider, who deploy or maintains networks, security solutions, communications solutions, hardware, software components, upgrades, etc., You are required to individually license each of Your customers.
PRESS <ENTER> TO CONTINUE:

5. RIGHTS, TITLE, AND INTEREST TO INTELLECTUAL PROPERTY. Unless as conveyed
herein, all rights, title, and interest in and to the Software, Documentation, and corresponding intellectual property (including without limitation any images, photographs, animations, video, audio, music, and text incorporated into the Software, the accompanying printed materials, and any copies of the Software) shall remain in SolarWinds or its suppliers or are publicly available. This EULA does not grant You any rights, title, or interest in or to any trademarks, service marks, or trade secrets of SolarWinds or its suppliers. The Software and Documentation are protected by the copyright and intellectual property laws of the United States and international copyright and intellectual property laws and treaties. All title, rights, and interest in and to content, which may be accessed through the Software ("Content"), is the property of the respective Content owner, shall be retained by the applicable Content owner, and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA gives You no rights to such

Content, including use of the same. All rights not expressly granted under this EULA are reserved by SolarWinds, its suppliers, or third parties.
6. DATA RIGHTS. SolarWinds agrees that the data and information (including without limitation, computer software, computer database, computer software documentation, specifications, design drawings, reports, blueprints, and the PRESS <ENTER> TO CONTINUE:

like) generated by the Software from Your proprietary data and information shall be and remain Your sole property. SolarWinds may collect and track non-personally identifiable information about You, including but not limited to Your IP address, the type of hardware You use, and the type of browser You employ, to assist with the necessary operation and function of the Software. SolarWinds reserves the right to compile, save, and use within the scope of SolarWinds' activities and to analyze any and all of Your data (registration data and use history). SolarWinds' use of any such data shall be for internal purposes only, including without limitation for the purposes of responding to Your requests for information, for contacting You, or providing You maintenance and support. Any such use of Your data will be treated as confidential information. SolarWinds may provide aggregated statistics about Your use of the Software to third parties, but such information will be aggregated so that it does not identify a particular individual or company.
7. LIMITED WARRANTY. SolarWinds warrants to You that for a period of thirty (30) days following delivery of the Software to You that the Software will perform substantially in conformance with the published Documentation. SolarWinds does not warrant that the Software will meet all of Your requirements or that the use of the Software will be uninterrupted or error-free. The foregoing warranty applies only to failures in operation of the Software that are reproducible in standalone form and does not apply to: PRESS <ENTER> TO CONTINUE:
(i) Software that is modified or altered by You or any third party that is not authorized by SolarWinds; (ii) Software that is otherwise operated in violation of this EULA or other than in accordance with the published Documentation; or (iii) failures that are caused by other software or hardware products. To the maximum extent permitted under applicable law, as SolarWinds and its supplier's entire liability, and as Your exclusive remedy for any breach of the foregoing warranty, SolarWinds will, at its sole option and expense, promptly repair or replace any medium or Software that fails to meet this limited warranty or, if SolarWinds is unable to repair or replace the medium or the Software, refund to You the applicable license fees paid upon return, if applicable, of the nonconforming item to SolarWinds. The warranty is void if failure of the Software has resulted from accident, abuse, or misapplication. Any replacement Software will be warranted for 30 days.
SOLARWINDS WARRANTS THAT THE SOFTWARE AND RELATED DOCUMENTATION DO NOT INFRINGE

ON ANY PATENTS, COPYRIGHTS OR TRADEMARKS OR CONSTITUTE MISAPPROPRIATION OF
THIRD PARTY PROPRIETARY INFORMATION.
EXCEPT AS EXPRESSLY STATED IN THIS SECTION, SOLARWINDS IS PROVIDING AND
LICENSING THE SOFTWARE TO YOU "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER
EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.
PRESS <ENTER> TO CONTINUE:

8. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW,
IN NO EVENT WILL SOLARWINDS BE LIABLE TO YOU FOR MORE THAN THE AMOUNT OF
LICENSE FEES THAT YOU HAVE PAID TO SOLARWINDS IN THE PRECEDING (12) TWELVE
MONTHS OR BE LIABLE TO YOU FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES,
INCLUDING LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL
DAMAGES, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE OR SOFTWARE
PROGRAMS, EVEN IF SOLARWINDS OR A DEALER AUTHORIZED BY SOLARWINDS HAD BEEN
ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
9. MISCELLANEOUS. If any provision of this EULA is held to be unenforceable, that shall not affect the enforceability of the remaining provisions. This EULA shall be governed by the laws of the State of Texas and of the United States, without regard to any conflict of laws provisions, except that the United Nations Convention on the International Sale of Goods shall not apply. You hereby consent to jurisdiction of the courts of both the state or federal courts of Texas.
10 COUNTERPARTS AND FACSIMILE SIGNATURE. This EULA may be executed in counterparts, each of which shall be deemed an original and all of which shall constitute one and the same instrument. The Parties may exchange signature pages by facsimile and such signatures shall be effective to bind the Parties. PRESS <ENTER> TO CONTINUE:

11. COMPLETE AGREEMENT. This EULA constitutes the entire agreement between the Parties and supersedes all prior or contemporaneous communications, agreements and understandings, written or oral, with respect to the subject matter hereof including without limitation the terms of any party EULA or any purchase order

issued in connection with this EULA. This EULA shall not be amended or modified except in a writing signed by authorized representatives of each party.
12. RESTRICTED RIGHTS. SolarWinds' Software is provided to non-DOD agencies with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the government is subject to the restrictions as set forth in subparagraph "C" of the Commercial Computer Software ? Restricted Rights clause at FAR 52.227-19. In the event the sale is to a DOD agency, the government's rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202. Manufacturer is SolarWinds Worldwide, LLC, 3711 South MoPac Expressway, Building Two Austin,Texas 78746.?
PRESS <ENTER> TO CONTINUE:

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): Y
==========
Choose Install Folder
---------- ---------
Where would you like to install?
Default Install Folder: /usr/local/contego/ContegoSPOP
ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAUL:
==========
Manager Name: : x.x.x.x
Manager Install Port (default 37890) : :
Manager Secure Port (default 37892) : :
==========
Manager Communication Summary
---------- ----------
You have entered the following Manager Communication settings:
Manager: x.x.x.x
Install Communications Port: 37890
Secure Communications Port: 37892
PRESS <ENTER> TO CONTINUE:

==========
Pre-Installation Summary
---------- ----------
Please Review the Following Before Continuing:
Product Name:

SolarWinds Log & Event Manager Agent
Install Folder:
/usr/local/contego/ContegoSPOP
Install Set:
Typical
Product Features:
Application,
Help
Disk Space Information (for Installation Target):
Required: 187,775,423 Bytes
Available: 20,594,324,480 Bytes
PRESS <ENTER> TO CONTINUE:

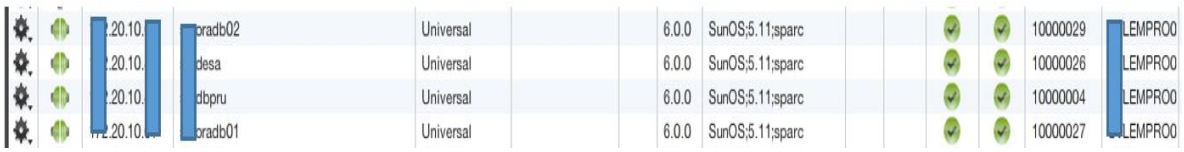
==========
Installing...

[==========|==========|==========|=====]
[----------|----------|----------|----------]
==========
Installation Complete

Congratulations. the SolarWinds Log & Event Manager Agent has been successfully installed to:
/usr/local/contego/ContegoSPOP
PRESS <ENTER> TO EXIT THE INSTALLER:
root@svrdesa:/home/admin#
root@svrdesa:/home/admin#

En la Figura 45 se muestran los dispositivos instalados con sistema operativo SunOS,5.11UNIX.

Figura 45. Agentes instalados UNIX.



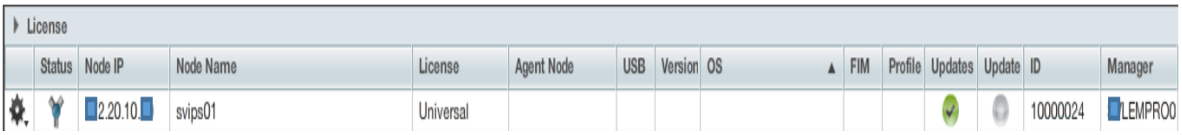
Fuente Herramienta Lem

Para la ANSPE se instala en los servidores de base de datos ORACLE en los ambientes de desarrollo y producción.

B.3 SISTEMAS OPERATIVOS PROPIOS DEL FABRICANTE

Para el caso de dispositivos de red o de seguridad que no permiten la instalación de agentes, la herramienta LEM cuenta con unos conectores que permiten realizar la transferencia de los logs del dispositivo al repositorio destinado permitiendo el almacenamiento y análisis de los mismos. Esto se efectúa habilitando él envió de SYSLOG o TRAPs de SNMP en una comunidad creada para enviar datos de forma segura, como se muestra en la Figura 46.

Figura 46. Conector de IPS.



Fuente Herramienta LEM

Entre los dispositivos que se realiza la conexión para este tipo de envío de logs se encuentra los dispositivos de McAfee: EmailGateway y Web Gateway.

ANEXO C

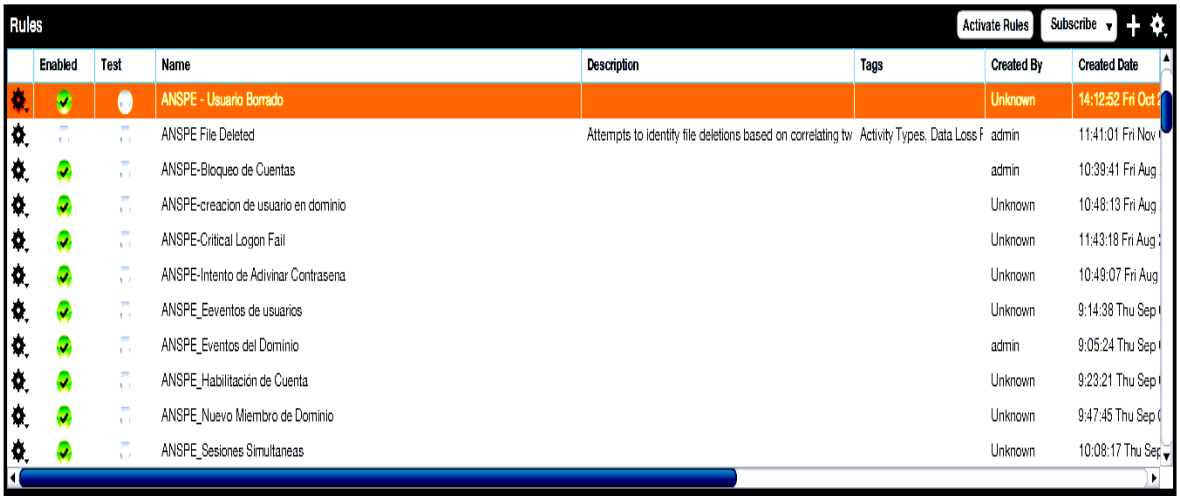
CONFIGURACIÓN DE REGLAS

C.1 ANÁLISIS DE LOGS Y CREACIÓN DE REGLAS

Luego de instalar los agentes y tener almacenados los Logs de los dispositivos, se debe configurar la herramienta LEM para generar reportes rápidos y continuos, con el fin de consultarlos de forma inmediata. En la Figura 47 se visualiza la configuración de reglas a realizar.

Figura 47. Configuración de reglas

.

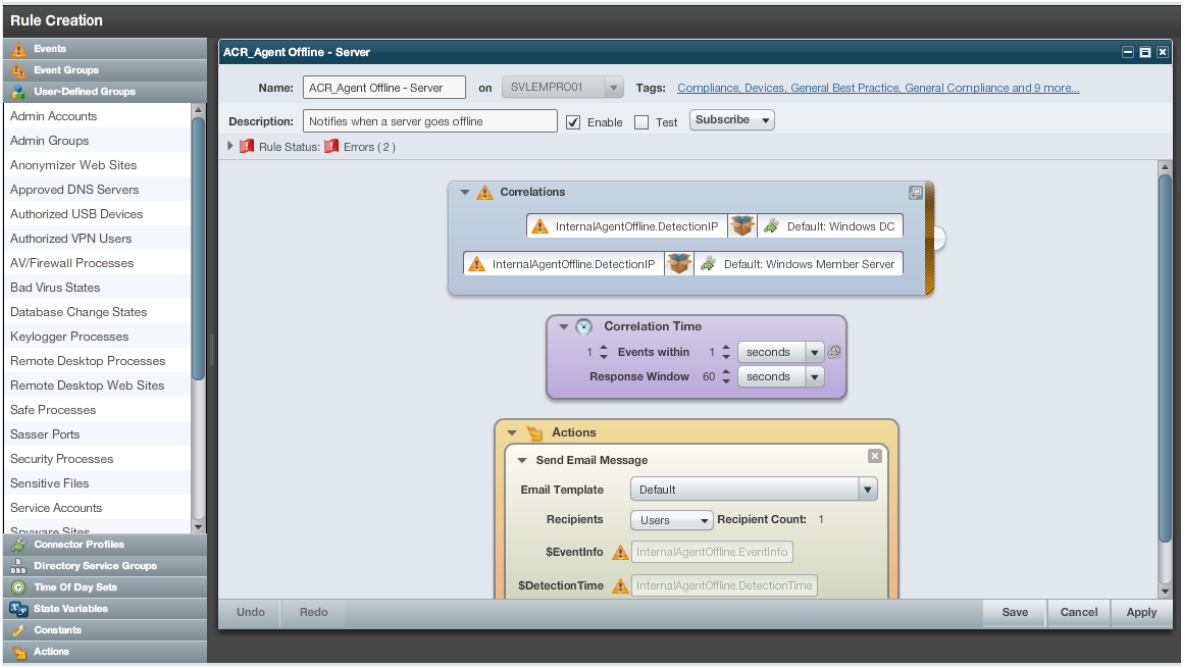


Fuente Herramienta LEM

LEM es una herramienta configurable que permite generar reportes, se basa en la programación orientada a objetos lo que facilita y hace más amigable para el administrador la creación de consultas, reglas y análisis de los logs almacenados.

De igual forma permite crear mediante código las reglas para generar los reportes o también ofrece la opción de reglas pre-configuradas en la herramienta, las cuales están orientas a la identificación de riesgos más comunes y eventos asociados de acuerdo a lo estipulado en las normas de seguridad de la información y a su vez pueden ser modificadas para ajustarse a las necesidades de la entidad. En la Figura 48 se encuentra un ejemplo de una regla configurada:

Figura 48. Regla de usuario borrado.



Fuente Herramienta LEM

La configuración al ser orientada a objetos permite que el administrador arrastre al panel principal (izquierda) lo que desea al panel de configuración (derecha), ya sea un elemento de correlación de tiempo o de acciones a tomar y ajuste la regla de forma tal que genere la información que necesita.

C.2 GENERAR REPORTES Y ACCIONES

La herramienta LEM cuenta con un módulo de reporte pre-configurados que permiten conocer el estado de los elementos seleccionados, así como reportes gráficos de un top de eventos registrados.

Lo anterior facilita generar reportes gerenciales y visuales para entornos administrativos o de monitoreo gráfico, como se muestra en la Figura 49.

Figura 49. Dashboard herramienta LEM.

Fuente Herramienta LEM

Los reportes gráficos permiten ser configurados de múltiples formas a mérito del administrador de la herramienta y ajustarlo a las necedades de la entidad.

Se pueden observar ambientes de top de eventos gráficos en forma de pie, barras puntos o cuadros de información.

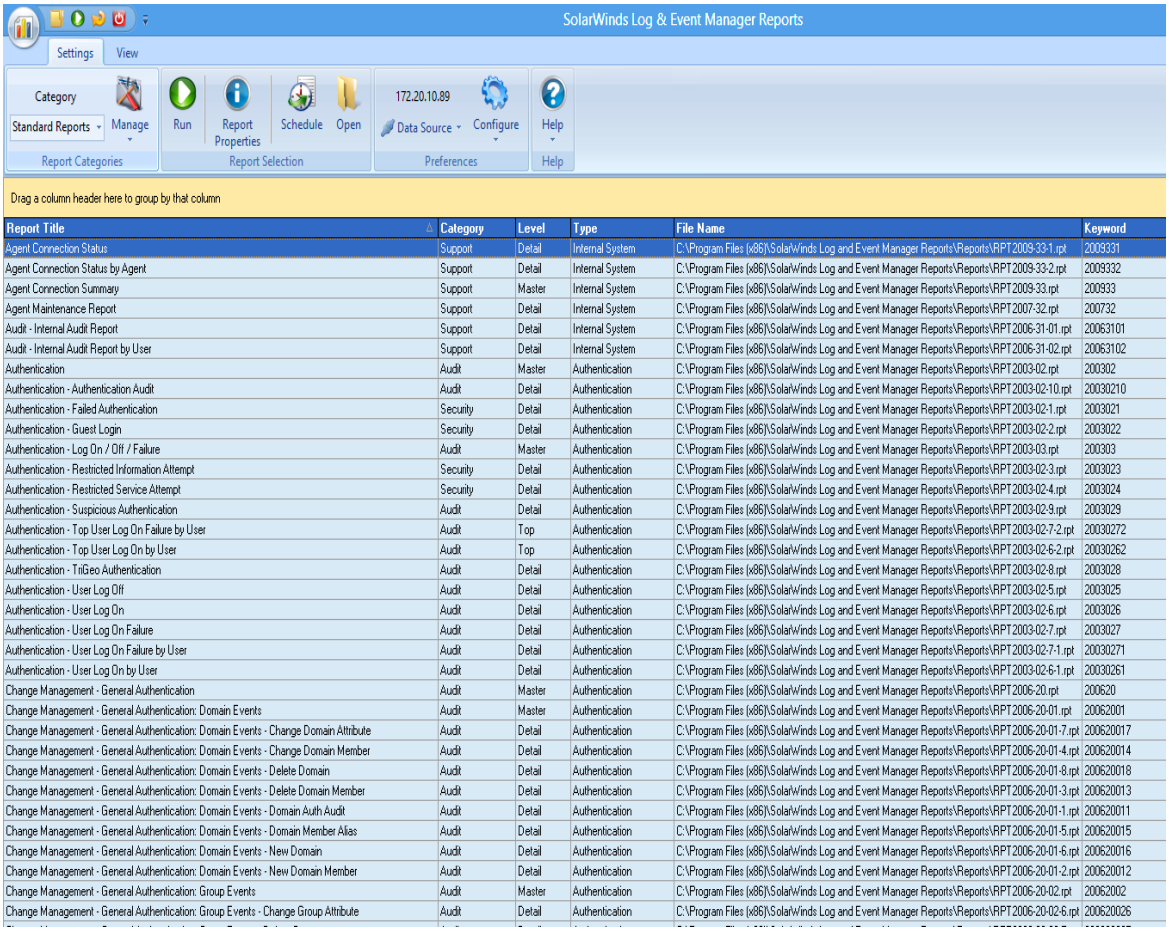
En la Figura 50 se puede mostrar el evento más relevante en el instante de tiempo en el que se observe el reporte:

Figura 50. Dashboard de reportes.

Fuente Herramienta LEM

De igual forma se cuenta con una herramienta de reportes llamada Log and Event Manager Reports, la cual contiene una base de datos extensa de reportes pre-configurados que pueden ser ajustados a las necesidades de la entidad. La Figura 51, muestra la interface gráfica de estos reportes.

Figura 51. Herramienta Log and Event Manager Reports.

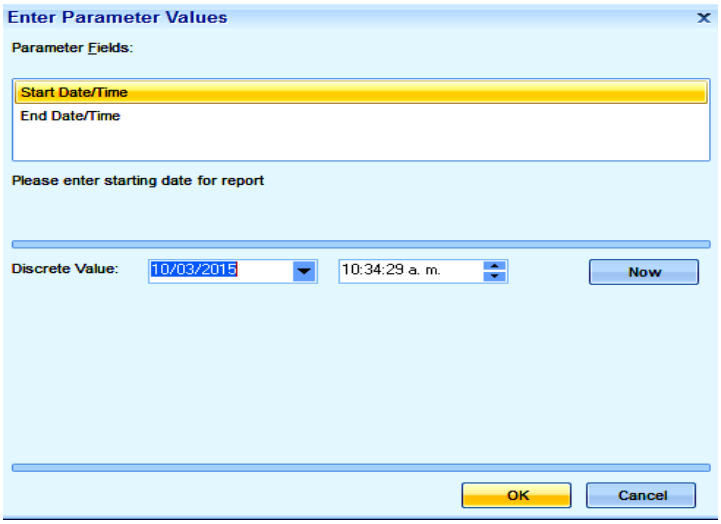


Report Title	Category	Level	Type	File Name	Keyword
Agent Connection Status	Support	Detail	Internal System	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2009-33-1.rpt	2009331
Agent Connection Status by Agent	Support	Detail	Internal System	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2009-33-2.rpt	2009332
Agent Connection Summary	Support	Master	Internal System	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2009-33.rpt	200933
Agent Maintenance Report	Support	Detail	Internal System	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2007-32.rpt	200732
Audit - Internal Audit Report	Support	Detail	Internal System	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-31-01.rpt	20063101
Audit - Internal Audit Report by User	Support	Detail	Internal System	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-31-02.rpt	20063102
Authentication	Audit	Master	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02.rpt	200302
Authentication - Authentication Audit	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-10.rpt	20030210
Authentication - Failed Authentication	Security	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-1.rpt	2003021
Authentication - Guest Login	Security	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-2.rpt	2003022
Authentication - Log On / Off / Failure	Audit	Master	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-03.rpt	200303
Authentication - Restricted Information Attempt	Security	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-3.rpt	2003023
Authentication - Restricted Service Attempt	Security	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-4.rpt	2003024
Authentication - Suspicious Authentication	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-9.rpt	2003029
Authentication - Top User Log On Failure by User	Audit	Top	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-7-2.rpt	20030272
Authentication - Top User Log On by User	Audit	Top	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-6-2.rpt	20030262
Authentication - TriGeo Authentication	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-8.rpt	2003028
Authentication - User Log Off	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-5.rpt	2003025
Authentication - User Log On	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-6.rpt	2003026
Authentication - User Log On Failure	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-7.rpt	2003027
Authentication - User Log On Failure by User	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-7-1.rpt	20030271
Authentication - User Log On by User	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2003-02-6-1.rpt	20030261
Change Management - General Authentication	Audit	Master	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20.rpt	200620
Change Management - General Authentication: Domain Events	Audit	Master	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-01.rpt	20062001
Change Management - General Authentication: Domain Events - Change Domain Attribute	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-01-7.rpt	200620017
Change Management - General Authentication: Domain Events - Change Domain Member	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-01-4.rpt	200620014
Change Management - General Authentication: Domain Events - Delete Domain	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-01-8.rpt	200620018
Change Management - General Authentication: Domain Events - Delete Domain Member	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-01-3.rpt	200620013
Change Management - General Authentication: Domain Events - Domain Auth Audit	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-01-1.rpt	200620011
Change Management - General Authentication: Domain Events - Domain Member Alias	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-01-5.rpt	200620015
Change Management - General Authentication: Domain Events - New Domain	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-01-6.rpt	200620016
Change Management - General Authentication: Domain Events - New Domain Member	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-01-2.rpt	200620012
Change Management - General Authentication: Group Events	Audit	Master	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-02.rpt	20062002
Change Management - General Authentication: Group Events - Change Group Attribute	Audit	Detail	Authentication	C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\Reports\RPT2006-20-02-6.rpt	200620026

Fuente Herramienta LEM

Al momento de seleccionar alguno de estos reportes se solicita la información del tiempo en el cual se va generar el reporte, lo cual se parametriza en la ventana de la Figura 52.

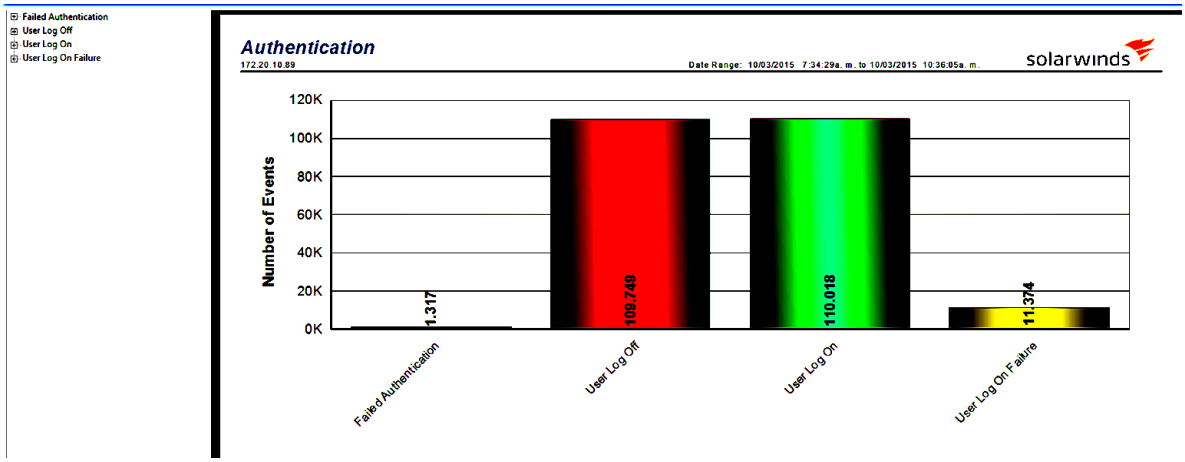
Figura 52. Parámetros del reporte.



Fuente Herramienta LEM

Los reportes generados se presentan en diferentes módulos como se muestra en la Figura 53, el primer informe es una gráfica con la cantidad de registros que se tiene del evento

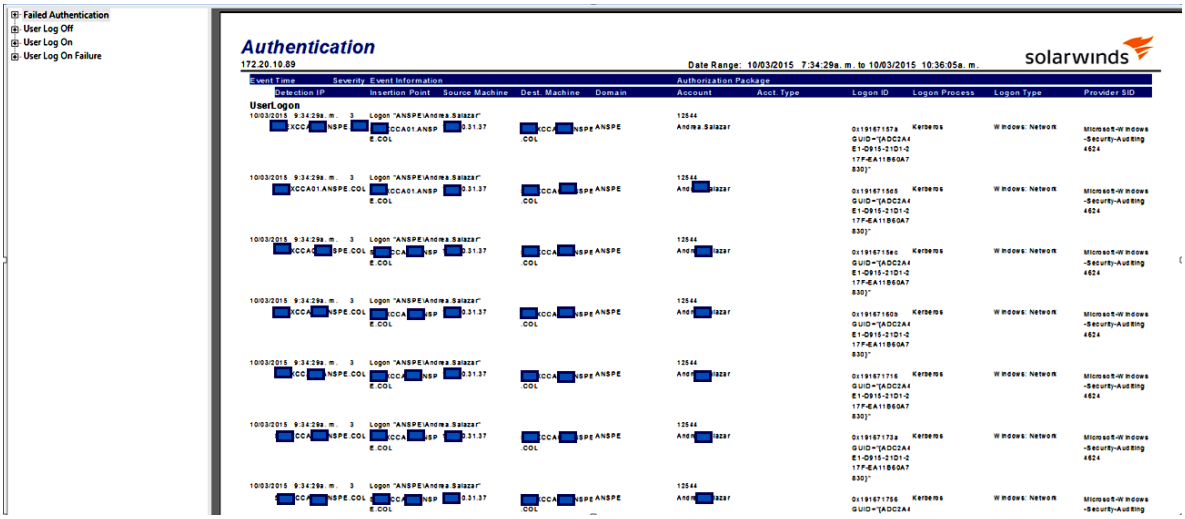
Figura 53. Entrega de reportes 1.



Fuente Herramienta LEM

En un segundo reporte que muestra en la Figura 54, se observa uno a uno los registros del evento consultado para generar el reporte.

Figura 54. Entrega de reportes 2.



Fuente Herramienta LEM